KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
INFORMACIJOS IR INFORMACINIŲ TECHNOLOGIJŲ SAUGA (6211BX008)

ADOMAS BAZINYS

IT SAUGOS POLITIKOS AUTOMATIZUOTO VALDYMO MODELIS

Baigiamasis magistro projektas

Vadovas
Prof. A. Venčkauskas

Kaunas, 2023

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
INFORMACIJOS IR INFORMACINIŲ TECHNOLOGIJŲ SAUGA (6211BX008)

ADOMAS BAZINYS

IT SAUGOS POLITIKOS AUTOMATIZUOTO VALDYMO MODELIS

Baigiamasis magistro projektas

Vadovas
Prof. A. Venčkauskas
(parašas) (data)

Recenzentas
Doc. Š. Grigaliūnas
(parašas) (data)

Studentas
A. Bazinys
(parašas) (data)

Kaunas, 2023

Kauno technologijos universitetas

Informatikos Fakultetas

Adomas Bazinys

IT saugos politikos automatizuoto valdymo modelis

Akademinio sąžiningumo deklaracija

Patvirtinu, kad mano, Adomo Bazinio, baigiamasis projektas tema „IT saugos politikos automatizuoto valdymo modelis“ 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)

Bazinys Adomas. IT saugos politikos automatizuoto valdymo modelis. Magistro baigiamasis projektas. Vadovas Prof. Algimantas Venčkauskas; Kauno technologijos universitetas, Informatikos fakultetas.

Studijų kryptis ir sritis (studijų krypčių grupė): Informatikos inžinerija (Informatikos mokslai).

Reikšminiai žodžiai: informacijos sauga, saugumo politika, automatizacija.

Kaunas, 2023. 107 p.

Santrauka

Šio baigiamojo projekto tikslas yra pasiūlyti universalų IT saugos politikos automatizuoto valdymo modelį, jį įgyvendinti ir ištirti. Tikslo įgyvendinimui keliami šie uždaviniai:

1. Išanalizuoti saugos politiką ir su ja susijusias problemas bei iššūkius;
2. Išanalizuoti rinkoje egzistuojančius IT saugos politikos valdymo įrankius ir prototipus;
3. Pasiūlyti ir sukurti IT saugos politikos automatizuoto valdymo modelį;
4. Įgyvendinti IT saugos politikos automatizuoto valdymo modelio prototipą;
5. Ištirti įgyvendintą IT saugos politikos automatizuoto valdymo modelio prototipą ir įvertinti jo veikimą.

Projektą sudaro penkios dalys: probleminės srities analizė, siūlomo modelio aprašymas, modelio prototipo įgyvendinimas, modelio prototipo testavimas (eksperimentai) ir išvados.

Lentelių skaičius (12 vnt.), paveikslų skaičius (60 vnt.), literatūros šaltinių skaičius (24 vnt.).

Bazinys, Adomas. Model for IT Security Policy Automated Management. Master's Final Degree Project. Supervisor Prof. Algimantas Venčkauskas; Faculty of Informatics, Kaunas University of Technology.

Study field and area (study field group): Informatics Engineering (Computing).

Keywords: information security, security policy, automation.

Kaunas, 2023. 107 p.

Summary

The aim of this final project is to propose, implement and investigate a universal model for the automated management of IT security policies. The following tasks are set for the implementation of the goal:

1. Analyze the security policy and related problems and challenges;
2. Analyze existing IT security policy management tools and prototypes on the market;
3. Propose and create an IT security policy automated management model;
4. To implement the prototype of the IT security policy automated management model;
5. Investigate the implemented prototype of the IT security policy automated management model and evaluate its performance.

The project consists of five parts: analysis of the problem area, description of the proposed model, implementation of the model prototype, testing of the model prototype (experiments) and conclusions.

Number of tables (12 units), number of pictures (60 units), number of literary sources (24 units).

Turinys

Lentelių sąrašas

Paveikslų sąrašas

Santrumpų ir terminų sąrašas

Santrumpos:

SANS (*SysAdmin, Audit, Network, and Security*) – organizacija, siūlanti informacijos saugumo ir kibernetinio saugumo mokymus ir sertifikavimą.
NIST (*National Institute of Standards and Technology*) – nacionalinis standartų ir technologijų institutas.
IDS (*Intrustion Detection System*) – atakų atpažinimo sistema.
SIEM (*Security Information and Event Management)* – saugos informacijos valdymas ir saugos įvykių valdymas.
ISO (*International Organization for Standardization*) – tarptautinė standartizacijos organizacija.
VPN (*Virtual Private Network*) – virtualus privatus tinklas.
KSP – kompiuterizuota saugumo politika.
GP – grupės politika (angl. *Group Policy*).
OV – organizacinis vienetas (angl. *Organizational Unit*).
DNS – srities vardų struktūra (angl. *Domain Name System*).

ĮVADAS

Mokslininkai sutaria, kad galutiniai kompiuterių vartotojai yra silpniausia informacinės saugos grandinės dalis. Saugos politika laikoma informacijos saugos valdymo ir organizavimo pamatu, kuris sušvelnina darbuotojų keliamas grėsmes [1]. Saugos politikos valdymas rankiniu būdu yra varginantis darbas. Siekiant saugos politikos atitikties valdymą paversti lengvesniu ir mažiau žmogiškųjų pastangų reikalaujančiu procesu iškeliamas šio baigiamojo darbo tikslas – sukurti IT saugos politikos automatizuoto valdymo modelį, jį įgyvendinti ir ištirti. Tikslo įgyvendinimui keliami žemiau išvardinti uždaviniai:

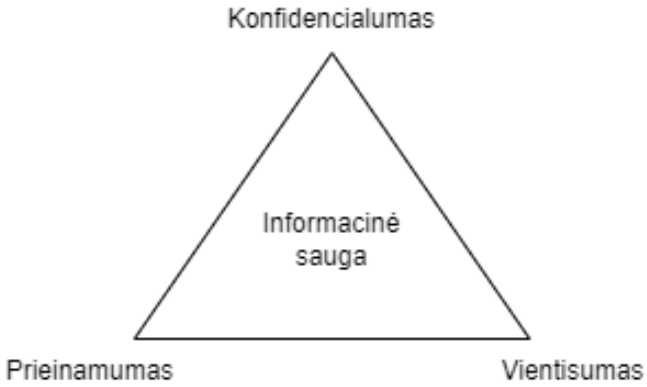
1. Išanalizuoti saugos politiką ir su ja susijusias problemas bei iššūkius;
2. Išanalizuoti rinkoje egzistuojančius IT saugos politikos valdymo įrankius ir prototipus;
3. Pasiūlyti ir sukurti IT saugos politikos automatizuoto valdymo modelį;
4. Įgyvendinti IT saugos politikos automatizuoto valdymo modelio prototipą;
5. Ištirti įgyvendintą IT saugos politikos automatizuoto valdymo modelio prototipą ir įvertinti jo veikimą.

Darbe naudojamos dvi sąvokos – saugos politika ir saugumo politika. Saugos politika laikoma organizacijos saugos politika bendrąja prasme, o saugumo politika – konkrečiomis taisyklėmis, įgyvendinančiomis tam tikrą saugumo reikalavimą.

1. SAUGOS POLITIKOS ĮGYVENDINIMO ANALIZĖ

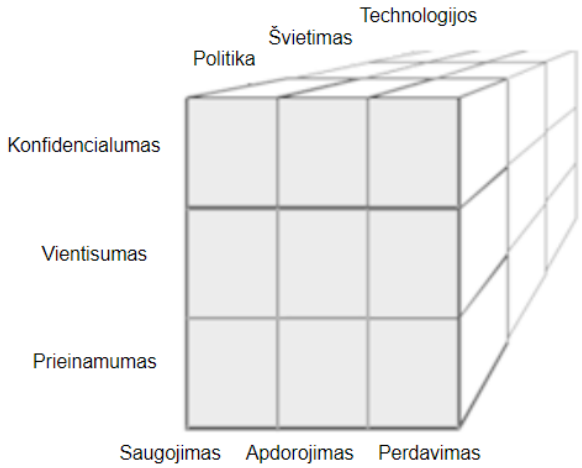
1.1. Saugumo politika

Saugumo politika yra taisyklė, kuria nusakomos elgesio organizacijoje normos: tai, kas yra priimtina ir nepriimtina darbuotojui dirbant su organizacijai priklausančiais informaciniais ištekliais [1]. Taigi, saugumo politikos tikslas yra įforminti ir aprašyti organizacijos IT infrastruktūros ir fizinės apsaugos metodikas, kuriomis siekiama apsaugoti organizacijos informacinių išteklių prieinamumą, konfidencialumą ir vientisumą. Visa tai įeina į informacinės saugos triadą, kuri yra pavaizduota 1.1 pav.



1.1 pav. Informacinės saugos triada

Egzistuoja skirtingų saugumo politikos apibrėžimų. Pagal SANS, saugumo politika yra *„ne kas kita, kaip gerai aprašyta strategija, skirta apsaugoti ir palaikyti prieigą prie tinklo bei jo išteklių“* [2]. Pagal NIST, saugumo politika yra - *„direktyvų, reglamentų, taisyklių ir praktikos visuma, nurodanti, kaip organizacija valdo, saugo ir platina informaciją“* [3]. 1991 metais John McCumber pristatė garsųjį saugos architektūros modelį, turintį tris dimensijas (sluoksnius) ir atrodantį kaip rubiko kubo žaislas. Modelis pavaizduotas 1.2 pav.



1.2 pav. *McCumber* kubo modelis

Pirmoji kubo dimensija primena apie būtinybę apsaugoti informacines sistemas ir atitinka 1.1 pav. pavaizduotą informacijos saugos triadą. Antroji kubo dimensija skirta duomenų apsaugai

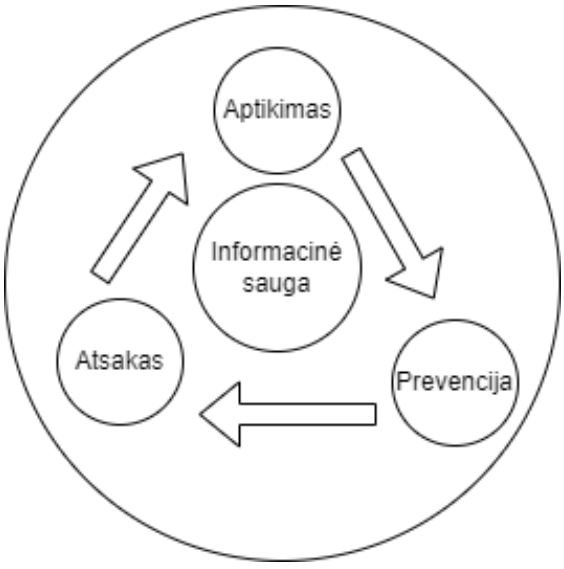
kiekvienoje įmanomoje stadijoje – saugojime (kietuosiuose diskuose, USB raktuose ir kt.), apdorojime, perdavime. Trečioji kubo dimensija apibrėžia priemones – politikas, švietimą, technologijas. Kiekvienas iš 27 langelių reiškia vieną konkrečią sritį, į kurią reikia atkreipti dėmesį, kad informacinė sistema būtų saugi. Pavyzdžiui, susikirtimas tarp vientisumo, technologijų ir saugojimo langelių rodo, kad reikia naudoti technologijas, siekiant apsaugoti duomenų vientisumą jų saugojimo metu [4]. Galima daryti prielaidą, kad McCumber modelis organizacijoms primena apie struktūrizuotą informacijos saugos politikos kūrimo metodą, padedantį kurti veiksmingas saugumo politikas, mažinančias neteisėtos prieigos prie išteklių ir informacijos nutekėjimo riziką.

1.2. Informacinės saugos procesas

Remiantis [5] informacinės saugos procesas yra sudarytas iš trijų dalių:

- **Saugos incidentų prevencija** – priemonės, kurių imamasi siekiant užkirsti kelią saugos incidentams. Šios priemonės gali apimti saugumo politikas, reguliarius saugos auditus ir darbuotojų informuotumo apie saugumą mokymus;
- **Saugos incidentų aptikimas** – procesas, kurio metu nustatomas saugos incidento atsiradimo faktas. Tam galima naudoti saugos stebėjimo įrankius, pvz., IDS, SIEM sistemas, taip pat rankiniu būdu stebėti sistemos žurnalus ir kitus rodiklius;
- **Atsakas į saugos incidentus** – veiksmų seka, kurios imamasi įvykus saugos incidentui. Tai apima tokius dalykus kaip incidento sustabdymas, kad būtų išvengta didesnės žalos, incidento analizė, siekiant nustatyti jo mastą ir sunkumą, ir veiksmų, skirtų incidento pasekmėms ištaisyti ir užkirsti kelią panašiems incidentams ateityje, ėmimasis. Įvykus incidentui, į jį turi būti atitinkamai reaguojama, remiantis incidentų valdymo plane pateiktomis instrukcijomis.

Informacinės saugos procesas grafiškai pavaizduotas 1.3 pav.



1.3 pav. Informacinės saugos procesas

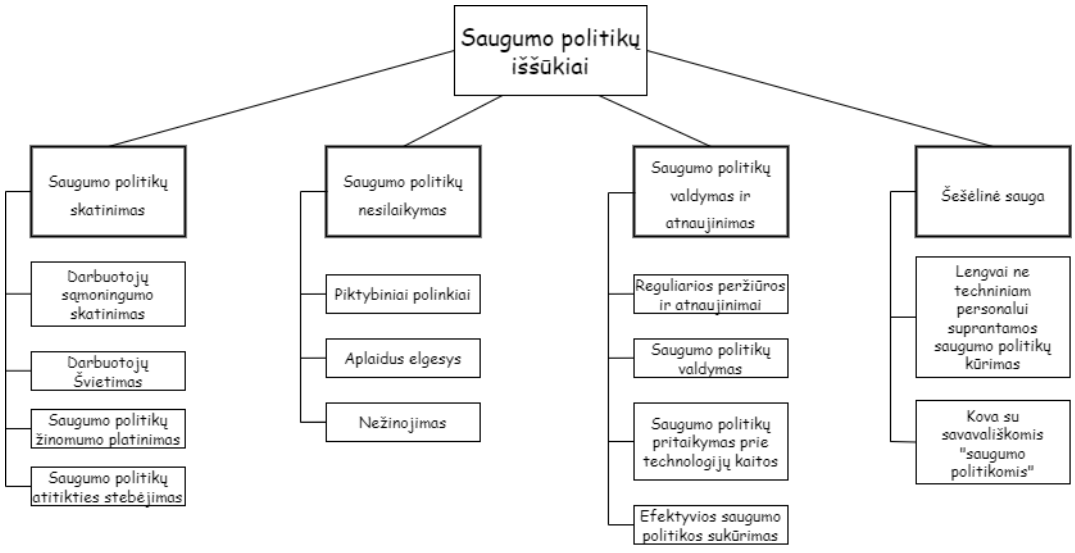
1.3. Informacinės saugos reikalavimai

Visapusiškas informacinės saugos reikalavimų supratimas vaidina svarbų vaidmenį kuriant tinkamą organizacijos poreikius atitinkančią informacijos saugos politiką. Pagal ISO, yra trys šaltiniai iš kurių gaunama būtiniausia informacija apie saugos reikalavimus:

- **Rizikos vertinimo**. Tai yra rizikų, galinčių turėti įtakos organizacijos gebėjimui pasiekti saugos tikslus, nustatymo, analizės ir įvertinimo procesas [6];
- **Sutartinių reikalavimų.** Tai yra organizacijos sutartyse su trečiosiomis šalimis apibrėžti reikalavimai. Šių reikalavimų nesilaikymas gali baigtis sutarties reikalavimų pažeidimu ir teisiniais ginčais [7];
- **Teisinių reikalavimų**. Jie atlieka labai svarbų vaidmenį vertinant riziką, nes organizacijos turi laikytis įvairių įstatymų ir taisyklių, apimančių duomenų privatumą, kibernetinę saugą, darbo vietos saugą. Pažeidus teisinius reikalavimus gali būti skiriamos teisinės ir finansinės nuobaudos, gali būti padaroma žala organizacijos reputacijai [8];
- **Organizacijos išteklių valdymo vizijos**, kuri apibrėžia tai, kas ir kaip dirbs su tam tikrais informaciniais ištekliais. [9].

1.4. Saugos politikos įgyvendinimo iššūkiai

Organizacijos skatindamos vartotojus laikytis saugos politikos susiduria su įvairiais iššūkiais. Siekiant išspręsti saugos politikos nesilaikymo problemą ir pagerinti atitiktį buvo pasitelkta daug techninių sprendimų bei metodų, įskaitant, bet neapsiribojant sistemų monitoringu, draudimais, autentifikacijos ir autorizacijos sprendimais. Tačiau net ir taikant pažangias technines priemones saugumo politikų atitiktis nėra garantuojama. M.Alotaibi, S. Furnell ir N.Clarke atlikto tyrimo metu priėjo prie išvados, kad egzistuoja keturių tipų saugumo politikų taikymo iššūkiai, pavaizduoti 1.4 pav.



1.4 pav. Saugumo politikų iššūkiai

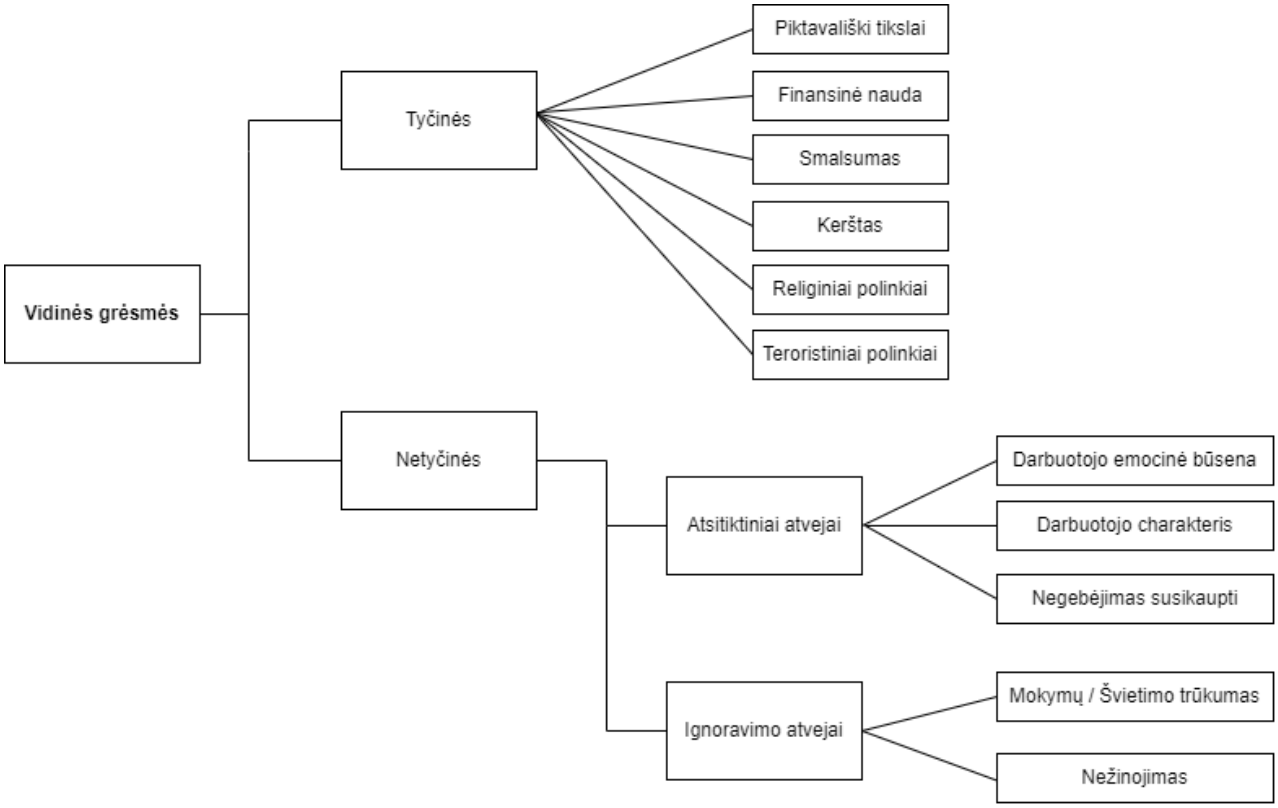
1.4.1. Saugos politikos skatinimas

Atlikto tyrimo metu paaiškėjo, kad tik nedaugelis organizacijų užsiėmė saugumo politikų kultūros į darbuotojų sąmonę diegimu. Autorius pabrėžia organizacijų būtinybę ne tik pasirūpinti

tinkamu saugumo politikų ir jų aprašymų pateikimu, tačiau ir bendru saugumo taisyklių laikymosi kultūros gerinimu organizacijoje [1].

1.4.2. Žmogiškasis faktorius

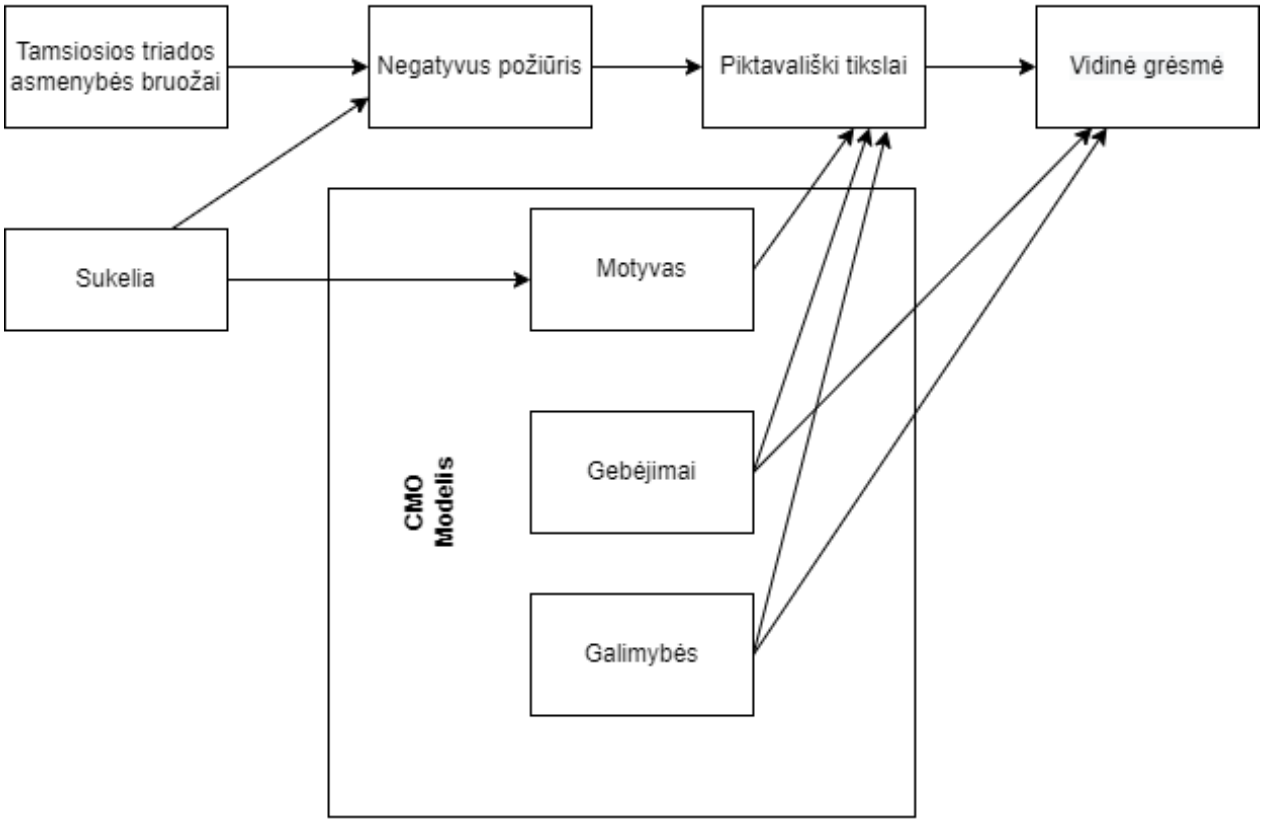
Informacinės saugos lygis organizacijose pirmiausiai priklauso nuo jos darbuotojų keliamos grėsmės. Neatsargumas, nežinojimas ar nurodymų nebuvimas gali iššaukti darbuotojų sukeltus informacinės saugos pažeidimus. Net ir turint oficialią saugos politiką, kai kurie darbuotojai apie tai nežino, o tai rodo būtinybę didinti darbuotojų informuotumą bei sukurti lengvai prieinamą ir visiems suprantamą informacijos saugos politiką. Nežinojimą, dėl kurio kyla žmogaus sukeltos rizikos, dažnai nulemia nepakankamas darbuotojų mokymas arba per didelis informacijos kiekis per trumpą laiko tarpą, ko pasekoje didelė dalis informacijos nėra įsisavinama. Toks žmogiškasis faktorius organizacijose iššaukia vidines grėsmes, kurios paprastai yra skirstomos į du tipus – tyčines ir netyčines. Grėsmių tipai pavaizduoti 1.5 pav.



1.5 pav. Žmogiškojo faktoriaus grėsmių tipai

Tyčinių grėsmių atveju darbuotojas turi piktavališkų paskatų ir yra motyvuotas pakenkti organizacijos saugai (šiuo atveju kenkėjas yra dar kitaip vadinamas vidiniu užpuoliku (angl. *Insider*). Remiantis CMO (angl. *Capability Motive Opportunity*) modeliu, vidiniam užpuolikui reikalingos trys sąlygos, kad jis galėtų piktnaudžiauti savo privilegijomis: motyvas, gebėjimai ir galimybės. Organizacijos darbuotojų motyvacija tyčia pakenkti organizacijos saugai dažniausiai būna finansinė nauda, smalsumas, kerštas, psichikos sutrikimai, religiniai ar teroristiniai polinkiai. Taip pat vidinį atakuotoją gali paveikti emocinė būsena (pyktis, baimė, stresas) [1]. Galimybės vidiniam užpuolikui atsiranda tada, kai sistemoje atrandama pažeidžiamumų, aptinkama spragų turinti konfigūracija. Gebėjimų veiksnys yra organizacijos darbuotojų techniniai įgūdžiai išnaudoti

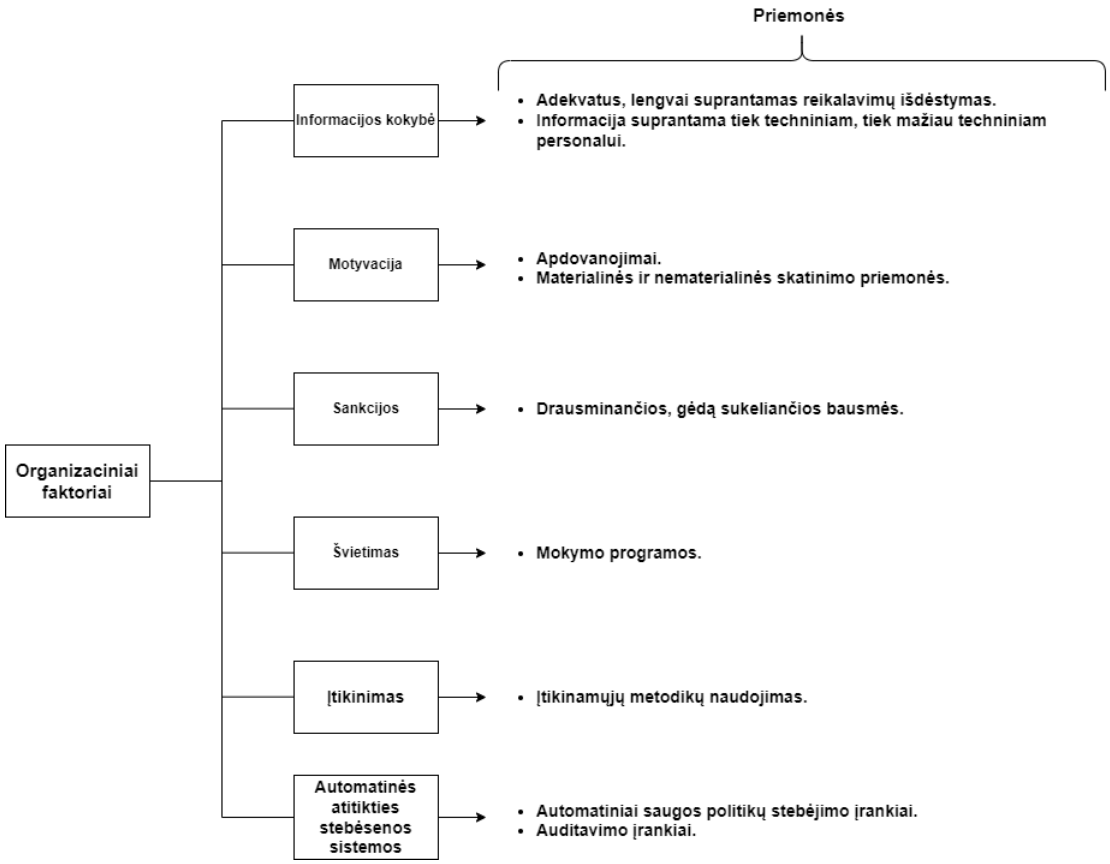
pasitaikiusias galimybes, į juos įeina konkrečių informacinių sistemų išmanymas, mokėjimas išnaudoti turimas prieigos teises bei pažeidžiamumus. 1.6 pav. pavaizduotas CMO modelis [11].



1.6 pav. CMO modelis

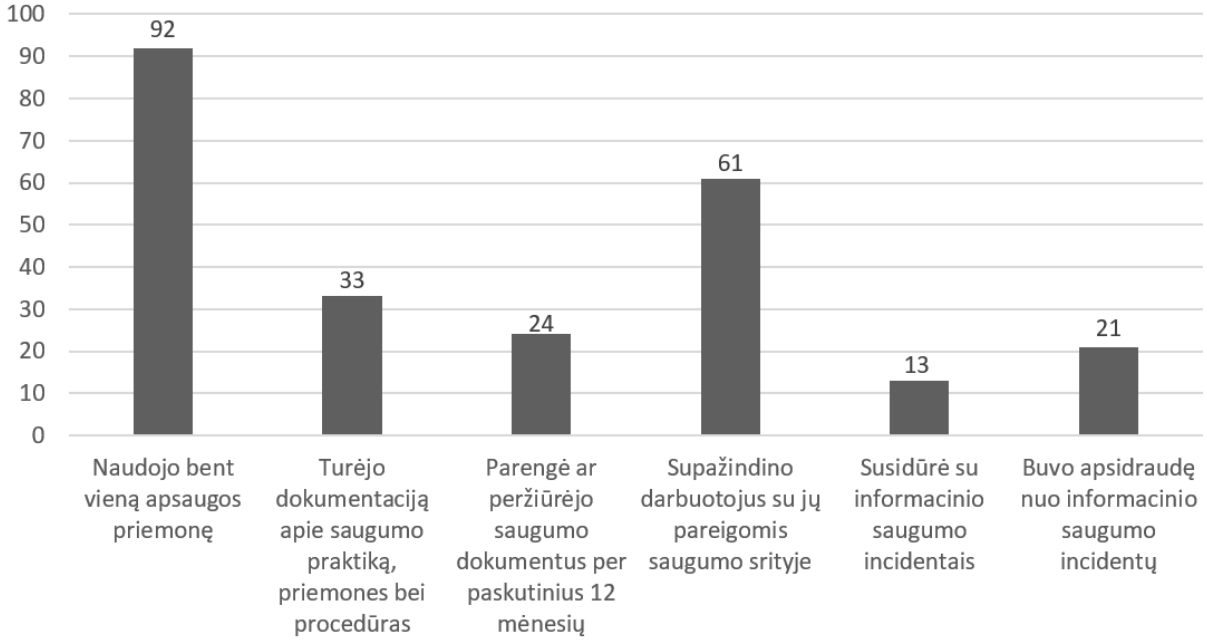
1.4.3. Organizacinis faktorius

Organizacinis faktorius atspindi organizacijos pastangas bei metodus teikti su saugos reikalavimais susijusią informaciją, motyvuoti, ugdyti personalo sąmoningumą laikytis saugumo politikų, bausti jų nesilaikančius, taip pat techninėmis priemonėmis stebėti saugos politikos atitikties lygį organizacijoje. Remiantis įvykdytų apklausų rezultatais padaryta išvada apie svarbiausius organizacinius faktorius, kurie pavaizduoti 1.7 pav. [1].



1.7 pav. Organizaciniai faktoriai

2019 metais atliktas *Eurostat* tyrimas parodė, kokių priemonių organizacijos ėmėsi siekiant užkirsti kelią kibernetiniams nusikaltimams. Matoma, kad tik 24 procentai organizacijų per paskutinius metus atnaujino arba peržiūrėjo su sauga susijusius dokumentus ar įstatus. 33 procentai apklaustųjų teigė turintys apibrėžtą saugos organizacijoje dokumentaciją, tačiau per paskutinius metus jos neperžiūrėję ir neatnaujinę. Tyrimo rezultatai grafiškai pavaizduoti 1.8 pav.



1.8 pav. Saugumo priemonių įvedimo organizacijose *Eurostat* tyrimo rezultatai

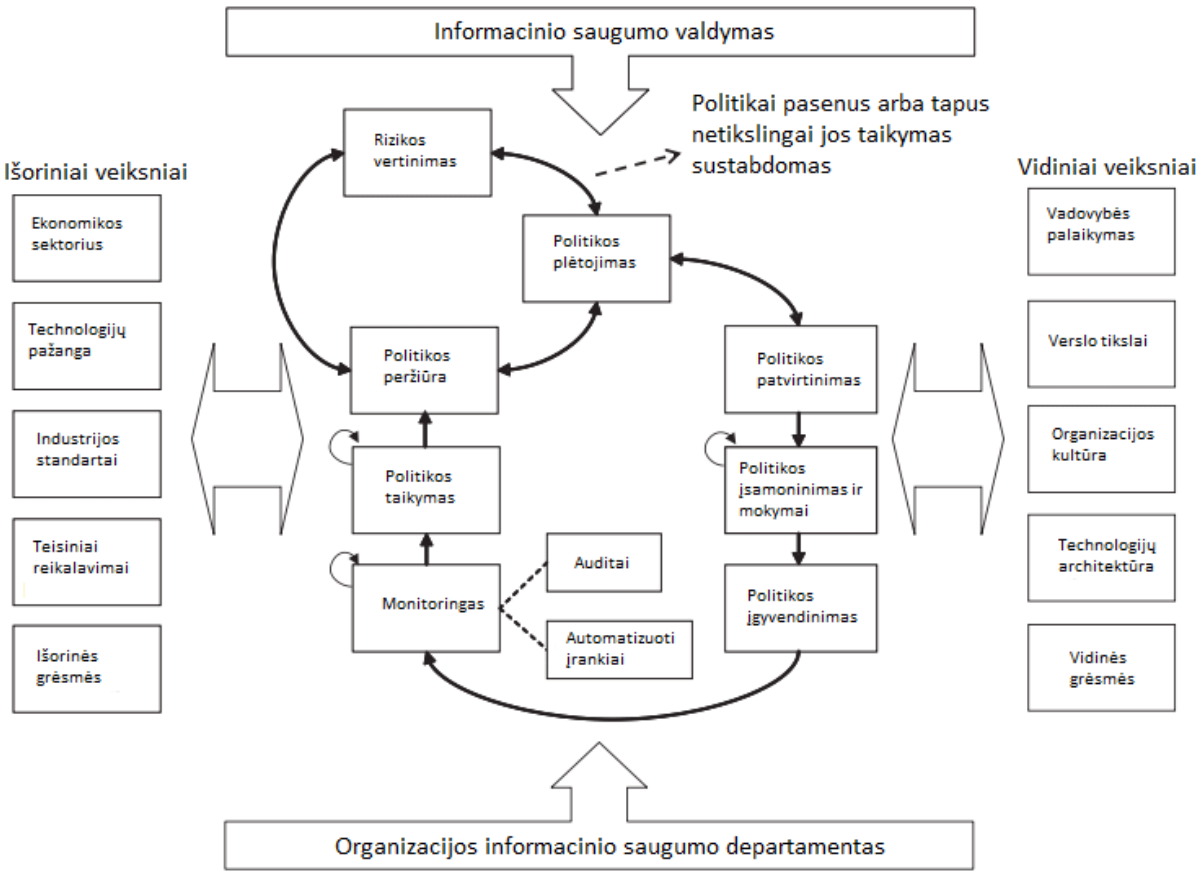
Taip pat matoma, kad 13 procentų apklaustų organizacijų atstovų teigė, kad per praeitus metus patyrė saugumo incidentų - nors tai ir nėra labai prasti rezultatai, tačiau labai tikėtina, kad tai gali būti atsitiktinės sėkmės rezultatas nesuvokiant tikrosios rizikos, kokius nuostolius organizacijos patirtų įvykus rimtesnei kibernetinei atakai [12].

1.4.4. Saugumo politikų valdymas

Saugumo politikų valdymo iššūkį puikiai atvaizduoja saugos politikos gyvavimo ciklo modelis, kurį pasiūlė profesorius Kenneth J. Knapp. Remiantis modeliu, yra dvi pagrindinės įtakos kategorijos, galinčios paveikti informacijos saugumo politikų valdymą:

- **Vidiniai veiksniai** – veiksniai, kurie kyla iš organizacijos vidaus, į juos įeina organizacijos kultūra ir struktūra, tikslai bei uždaviniai, ištekliai ir darbuotojų elgesys. Pavyzdžiui, organizacijos kultūra skatinanti saugumo sąmoningumą ir atsakomybę gali teigiamai paveikti saugos politikos kūrimą ir įgyvendinimą. Kita vertus, organizacijos išteklių stoka ar atsainus vadovybės požiūris į saugą gali neigiamai paveikti saugos politikos įgyvendinimą;
- **Išoriniai veiksniai** – veiksniai, kurie kyla iš už organizacijos ribų, pvz., teisės aktai ir reglamentai, pramonės standartai. Pavyzdžiui, naujas asmens duomenų apsaugos reglamentas gali reikalauti atnaujinti saugos politiką.

1.9 pav. pavaizduotas saugos politikos gyvavimo ciklo modelis.



1.9 pav. Saugos politikos gyvavimo ciklo modelis

Centrinė modelio dalis atvaizduoja informacijos saugumo politikos procesą ir jo sudedamuosius žingsnius, kuriuos pagrinde sudaro poreikio remiantis išoriniais bei vidiniais veiksniais tam tikrai

saugumo politikai atsiradimas (jos inicijavimas), plėtojimas, patvirtinimas, įgyvendinimas, taikymas, monitoringas bei periodinė peržiūra. Centrinė modelio dalis yra tikroji šio modelio esmė, nes ji atspindi tikrąjį informacijos saugumo politikos kūrimo ir įgyvendinimo procesą. Šis procesas turi būti gerai suplanuotas, gerai vykdomas ir nuolat atnaujinamas, siekiant užtikrinti, kad politika išliktų veiksminga kintant vidiniams ir išoriniams veiksniams. Svarbu paminėti, kad vykstant technologijų raidai, keičiantis saugos aktualijomis kai kurios politikos bėgant laikui gali tapti nebeaktualios, tokiu atveju jos pašalinamos iš organizacijos saugos dokumento ir jų taikymas organizacijoje yra sustabdomas [10].

1.4.5. Šešėlinė sauga

Šešėlinės saugos iššūkis slypi darbuotojų pasąmonėje. Tarp organizacijos darbuotojų neretai vyrauja įsitikinimas, kad jų saugos reikalavimų laikymasis ar pastangos jų laikytis trukdo darbui arba daro neigiamą įtaką darbo produktyvumui. Pavyzdžiui, aukšto sudėtingumo lygio slaptažodžio politiką daliai darbuotojų gali būti sunku jį prisiminti, todėl jį gali laikyti užrašytą ant lapuko ir priklijuotą prie monitoriaus. Tai yra vadinama šešėline sauga. Organizacijos noras apsaugoti darbuotojų įrenginius sudėtingais slaptažodžiais iššaukia neigiamą darbuotojų elgesį slaptažodžių saugos atžvilgiu – slaptažodžių laikymą daugumai prieinamoje vietoje. Pernelyg sudėtinga informacijos saugumo politika gali neužtikrinti aukšto saugos lygio organizacijoje, nes darbuotojai dažnu atveju bando rasti būdų, kaip apeiti sudėtingus, pasak jų nereikalingus procesus [1].

1.5. Saugumo politikų lygiai

Saugumo politikos yra skirstomos į du lygius: aukšto lygio saugumo politiką ir žemo lygio saugumo politiką. Aukšto lygio saugumo politika atspindi saugumo problemas ir tikslus aukščiausiu abstrakcijos lygiu. Pavyzdžiui, organizacija nustato informacijos šaltinio svarbą ir paskiria darbuotoją, atsakingą už šio šaltinio apsaugą. Antra, žemo lygio saugumo politika vadovaujasi aukšto lygio saugumo politika, kad būtų sumažinta aukštesnio lygio saugumo politikoje apibrėžto ištekliaus keliamos grėsmės tikimybė. Kitaip tariant, žemo lygio saugumo politika sprendžia konkrečias problemas ir apibrėžia konkrečias atsakomąsias priemones prieš grėsmes. Pavyzdžiui, aukšto lygio saugumo politika bylotų apie tai, kad reikia rūpintis slaptažodžių sauga. Tuo tarpu žemo lygio saugumo politika apie tai, kad darbuotojams privaloma keisti slaptažodžius kas tam tikrą nustatytą skaičių dienų. 1.10 pav. yra saugumo politikų lygių hierarchija.

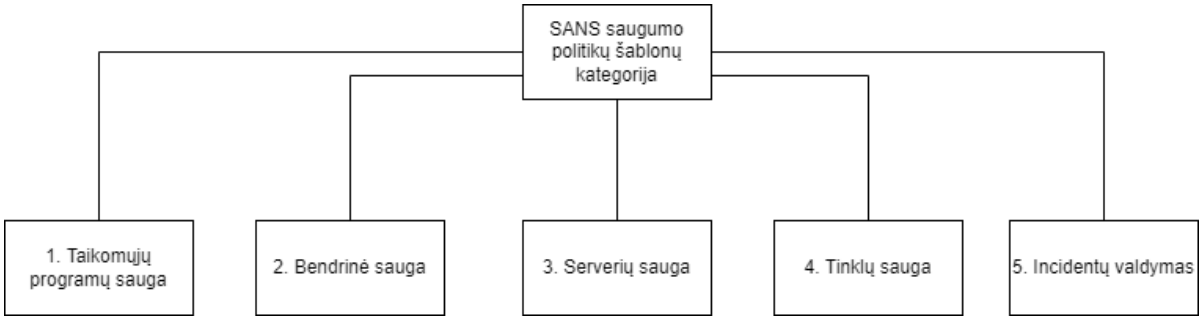
1.10 pav. Saugumo politikų lygių hierarchija

Priemonės šioje hierarchijoje yra techniniai įrankiai tikrinantys ir užtikrinantys žemo lygio saugumo politikos atitiktį ir tokiu būdu savo dalimi užtikrindami, kad aukšto lygio saugumo

politikos yra laikomasi. Aukšto lygio saugos politikos yra daug lengviau suprantamos ne techniniam personalui, todėl naudojant šį saugumo politikų skirstymą yra daug lengviau daryti pranešimus vadovybei apie visuotinį saugos lygį organizacijoje [13].

1.6. Saugumo politikos pagal SANS

SANS instituto sukurti ir viešai prieinami saugumo politikos šablonai padeda organizacijoms įgyvendinti savo saugos politiką. SANS nemokamai siūlo informacijos saugumo politikos šablonus, kurie yra suskirstyti į 5 kategorijas, pavaizduotas 1.11 pav..

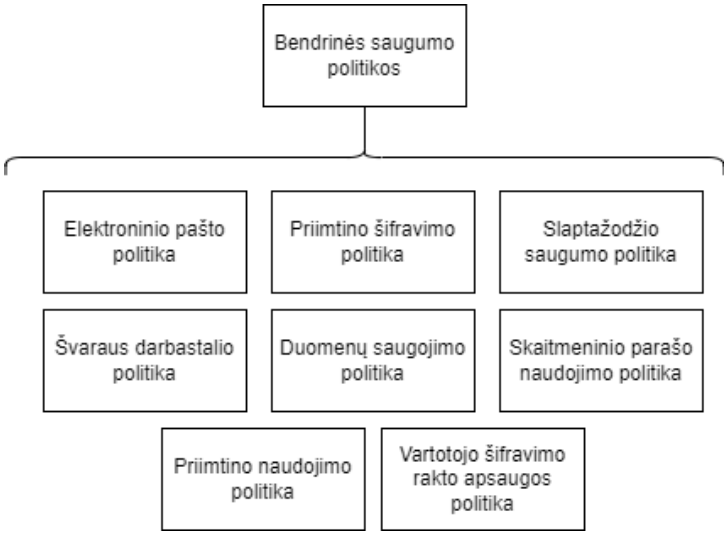


1.11 pav. SANS saugumo politikų šablonų kategorijos [15]

SANS politikų šablonai turi nustatytą struktūrą – politikos apžvalga, tikslas, taikymo sritis, politikos aprašymas, politikos atitikties tikrinimo būdai bei su politika siejami standartai bei procesai. Kiekviena organizacija gali naudoti ir taikyti šiuos šablonus, tačiau svarbu pabrėžti, jog bet kurio šablono paėmimas ir pritaikymas organizacijai jo nekoreguojant nėra naudingas, nes kiekviena organizacija turi individualius saugai keliamus reikalavimus. Sekančiuose skyreliuose bus pristatyti SANS saugumo politikų tipai bei jų pavyzdžiai [14].

1.6.1. Bendrinės saugumo politikos

Šiame skyrelyje pateikiamos bendrinių saugumo politikų pavyzdžiai [15].



1.12 pav. Bendrinių saugumo politikų šablonų tipai pagal SANS

1.1 lentelė. Bendrinės saugumo politikos

Žemo lygio saugumo politika	Politikos tipas	Atitikties tikrinimas / įgyvendinimas
Organizacijos el. pašto paskyros naudojimas slaptažodžių siuntimui, žeidžiantiems, grandininiams laiškams, taip pat kitais ne su organizacijos veikla susijusiais tikslais yra draudžiamas.	**Elektroninio pašto politika**	• Įeinančių ir išeinančių laiškų siuntėjų bei gavėjų kontrolė (viena iš opcijų - ne organizacijai priklausančių el. pašto adresų eismo blokavimas); • Laiškų turinio filtravimas (pagal laiške esančius tam tikrus raktinius žodžius blokuoti išeinantį laišką). Tokios filtravimo galimybės egzistuoja visose el. pašto programinėse įrangose – Office 365, Microsoft Exchange, GFI MailEssentials, TrendMicro ir daug kitų. Politikos atitiktis periodiškai tikrinama audito ir atsitiktinių patikrų metu.
Visi serveriai ir programos, naudojantys SSL arba TLS, turi turėti patikimo teikėjo pasirašytus sertifikatus.	**Priimtino šifravimo politika**	Apriboti galimybę komunikuoti su programomis, serveriais, neturinčiais patikimų teikėjų pasirašytų sertifikatų. Politikos atitiktis periodiškai tikrinama audito ir atsitiktinių patikrų metu.
Organizacijos darbuotojų paskyrų slaptažodžiai turi būti bent dvylikos simbolių ilgio, juose turi būti panaudotas bent vienas specialusis simbolis (pvz., !@#$%^&*) bei didžiosios ir mažosios raidės. Slaptažodžiai turi būti keičiami bent kartą per 90 dienų.	**Slaptažodžių saugumo politika**	Slaptažodžių saugumo politikos gali būti įgyvendinamos ir tikrinamos naudojant Active Directory sistemą. Politikos atitiktis periodiškai tikrinama audito metu.
Organizacijos darbuotojai palikdami darbo vietą privalo užrakinti kompiuterį.	**Švaraus darbastalio politika**	Politikos atitiktis tikrinama audito ir atsitiktinių patikrų metu.
Prieiga prie fizinių duomenų laikmenų (atminties raktų, išoriniai diskų), saugančių riboto naudojimo informacija bei kitą organizacijos informacinį turtą turi būti apribota ir apsaugota naudojant užrakintas spintas ar seifus.	**Duomenų saugojimo politika**	Politikos atitiktis periodiškai tikrinama audito metu arba įvykus reikšmingiems pokyčiams.
Organizacijos darbuotojai yra atsakingi už savo privataus rakto apsaugą, naudojamo skaitmeniniams parašams ir negali juo dalintis su kitais asmenimis.	**Skaitmeninio parašo naudojimo politika**	Politika įgyvendinama edukuojant ir rengiant mokymus organizacijos darbuotojams, ribojant prieigą prie sistemų atsakingų už privačių raktų generavimą ir atnaujinimą, vykdant privačių raktų, naudojamų skaitmeniniams parašams rotaciją. Politikos atitiktis periodiškai tikrinama audito ir atsitiktinių patikrų metu.
Prieiga prie organizacijos išteklių ne darbo valandų metu yra draudžiama.	**Priimtino naudojimo politika**	Politika įgyvendinama Active Directory sistemoje apribojant prieigą prie išteklių ne darbo valandų metu. Politikos atitiktis periodiškai tikrinama audito metu arba įvykus reikšmingiems pokyčiams.
Visi slaptažodžiai ar slaptafrazės, skirti apsaugoti privačius šifravimo raktus, turi atitikti organizacijos nustatytus sudėtingumo ir ilgio reikalavimus.	**Vartotojo šifravimo rakto apsaugos politika**	Taip pat kaip ir slaptažodžių apsaugos politikoje.

1.6.2. Serverių saugumo politikos

Šiame skyrelyje pateikiami serverių saugumo politikų pavyzdžiai [15].

1.13 pav. Serverių saugumo politikų šablonų tipai pagal SANS

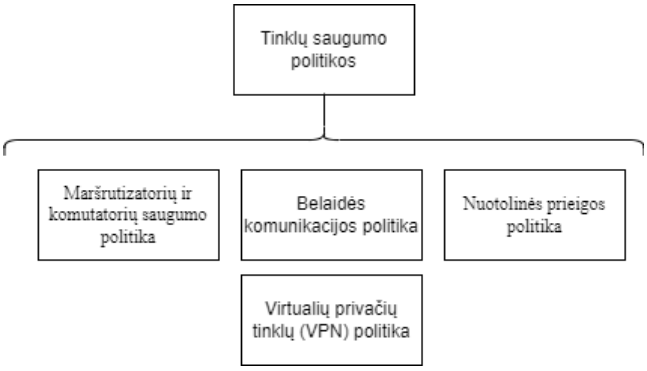
1.2 lentelė. Serverių saugumo politikos

Žemo lygio saugumo politika	**Politikos tipas**	**Atitikties tikrinimas / įgyvendinimas**
Serveriai, turintys prieigą prie konfidencialių informacinių išteklių, turi žurnalizuoti informaciją apie tai, kas kokią veiklą ir kada vykdė bei koks buvo veiklos vykdymo rezultatas.	**Įvykių žurnalizavimo standartai**	Auditų metu tikrinama SIEM, IDS, IPS ir kitų sistemų įvykių žurnalizavimo konfigūracija.
Kiekviena programa ir asmuo, dirbantis su duomenų baze privalo turėti unikalius duomenų bazės prisijungimus. Dalijimasis prisijungimais su kitomis programomis ar asmenimis yra griežtai draudžiamas.	**Duomenų bazių prisijungimo duomenų politika**	Politika įgyvendinama rengiant mokymus apie prisijungimo duomenų dalijimosi riziką, įdiegiant dviejų faktorių autentifikacijos sprendimus, periodiškai peržiūrint prieigos teises prie išteklių. Politikos atitiktis periodiškai tikrinama audito metu.
Prievadų nuskaitymai, brukalų (angl. S*pam Traffic*) generavimas ir kitos panašios veiklos prieš organizacijos DMZ zonoje esančius įrenginius yra draudžiamos.	**Laboratorijų saugumo politika**	• Ugniasienės prieš demilitarizuotą zoną turėjimas (privaloma); • Tinklo srauto stebėjimas ir įtartinų IP adresų blokavimas; • Naudotis brukalų filtravimo sprendimais (angl. Spam Filtering), integruotais į el. pašto serverius (pavyzdžiui SpamAssassin). Politikos atitiktis periodiškai tikrinama audito metu tikrinant konfigūraciją. Užtikrinama naudojant SCCM (angl. System Center Configuration Manager) sistemą, konkrečiai

		programinės įrangos centro (angl. Software Center) funkciją, kurioje aiškiai apibrėžiama domeno vartotojams leidžiamų naudoti programų aibė. Politikos atitiktis periodiškai tikrinama audito metu.
Instaliuojama trečiųjų šalių programinė įranga turi būti patvirtinta IT departamento.	**Programinės įrangos diegimo politika**	Užtikrinama naudojant SCCM (angl. System Center Configuration Manager) sistemą, konkrečiai programinės įrangos centro (angl. Software Center) funkciją, kurioje aiškiai apibrėžiama domeno vartotojams leidžiamų naudoti programų aibė. Politikos atitiktis periodiškai tikrinama audito metu.
Nurašant nebereikalingą įrangą, visi duomenys, įskaitant failus ir licencijuotą programinę įrangą, turi būti pašalinti iš nurašomo įrenginio.	**Įrangos nurašymo politika**	Politika įgalinama dokumentuojant įrangos eksploatavimo nutraukimo veiklą ir duomenų iš įrenginių pašalinimo procesus. Politikos atitiktis periodiškai tikrinama audito metu.
Privilegijuota prieiga prie serverių turi būti vykdoma šifruotais kanalais naudojant SSH (angl. *Secure Shell*).	**Serverių saugumo politika**	Serveriai turi būti sukonfigūruoti taip, kad prieiga prie jų būtų įmanoma tik saugiu SSH kanalu. Politikos atitiktis periodiškai tikrinama audito metu tikrinant konfigūraciją.

1.6.3. Tinklo saugumo politikos

Šiame skyrelyje pateikiami tinklo saugumo politikų pavyzdžiai [15].



1.14 pav. Tinklo saugumo politikų šablonų tipai pagal SANS

1.3 lentelė. Tinklo saugumo politikos

Žemo lygio saugumo politika	Politikos tipas	Atitikties tikrinimas / įgyvendinimas
Maršrutizatorių konfigūracijoje turi būti draudžiamos visos nešifruotu ryšiu veikiančios paslaugos kaip Telnet (23 prievadas), FTP (21 prievadas).	**Maršrutizatorių ir komutatorių saugumo politika**	Politikos atitiktis tikrinama audito metu peržiūrint ugniasienės konfigūraciją.
Organizacijos darbuotojai turi būti automatiškai atjungti nuo VPN tinklo po trisdešimties neveiklumo minučių (ping arba kiti dirbtiniai tinklo procesai negali būti naudojami norint išlaikyti prisijungimą).	**Virtualių privačių tinklų politika**	Politikos atitiktis tikrinama audito metu peržiūrint VPN serverio konfigūraciją.
Nuotolinė prieiga prie organizacijos įrenginių galima tik prisijungus prie VPN serverio.	**Nuotolinės prieigos politika**	Politikos atitiktis tikrinama audito metu peržiūrint VPN serverio konfigūraciją.

1.7. Saugumo politikų automatizuoto valdymo įrankiai

1.7.1. AlgoSec produktų linija

AlgoSec yra programinė įranga padedanti organizacijoms užtikrinti tinklo saugą automatizuojant organizacijos tinklo saugos politiką. AlgoSec veikia su tokiais įrenginiais kaip tinklo užkardos, maršrutizatoriai, VPN serveriai. Pagrindiniai AlgoSec produktų linijos tikslai - valdyti tinklo saugos konfigūraciją, identifikuoti pažeidžiamumus, atlikti tinklo saugos politikos testavimą maksimaliai sumažinant administracines išlaidas [16].

1.15 pav. AlgoSec logotipas

AlgoSec produktų liniją sudaro:

- AlgoSec Firewall Analyzer – įrankis, skirtas padėti tinklo saugos komandoms valdyti ir optimizuoti užkardos politiką. Įrankis analizuoja esamą užkardų taisyklių bazę, kad nustatytų nenaudojamas, pasikartojančias arba pasenusias taisykles. Įrankis įgyvendina vieningą platformą ugniasienės taisyklių analizei palaikydamas įvairių gamintojų kaip Cisco, Check Point, Palo Alto Networks, Juniper ir Fortinet ugniasienės programinę įrangą [17];
- AlgoSec FireFlow – įrankis, naudojamas automatizuoti tinklo saugos politikos keitimo valdymo procesą. Tai padeda tinklo saugos komandoms supaprastinti ir automatizuoti saugos politikos pakeitimo užklausų, projektavimo, patvirtinimo ir įgyvendinimo procesus [18];
- AlgoSec CloudFlow – įrankis, skirtas valdyti tinklo saugos politiką debesijos ir hibridinėse aplinkose, įskaitant Amazon Web Services (AWS), Microsoft Azure, Google Cloud ir kt [19].

1.7.2. Tufin Orchestration Suite įrankis

Tufin Orchestration Suite yra programinės įranga, naudojama tinklo saugos politikos valdymui įvairių gamintojų aplinkose. Tai centralizuota valdymo priemonė, skirta valdyti ugniasienės strategijas, saugos grupes, maršrutizatorius, šakotuvus, apkrovos balansavimo priemones ir kitus tinklo įrenginius.

1.16 pav. Tufin logotipas

Tufin Orchestration Suite produktų liniją sudaro [20]:

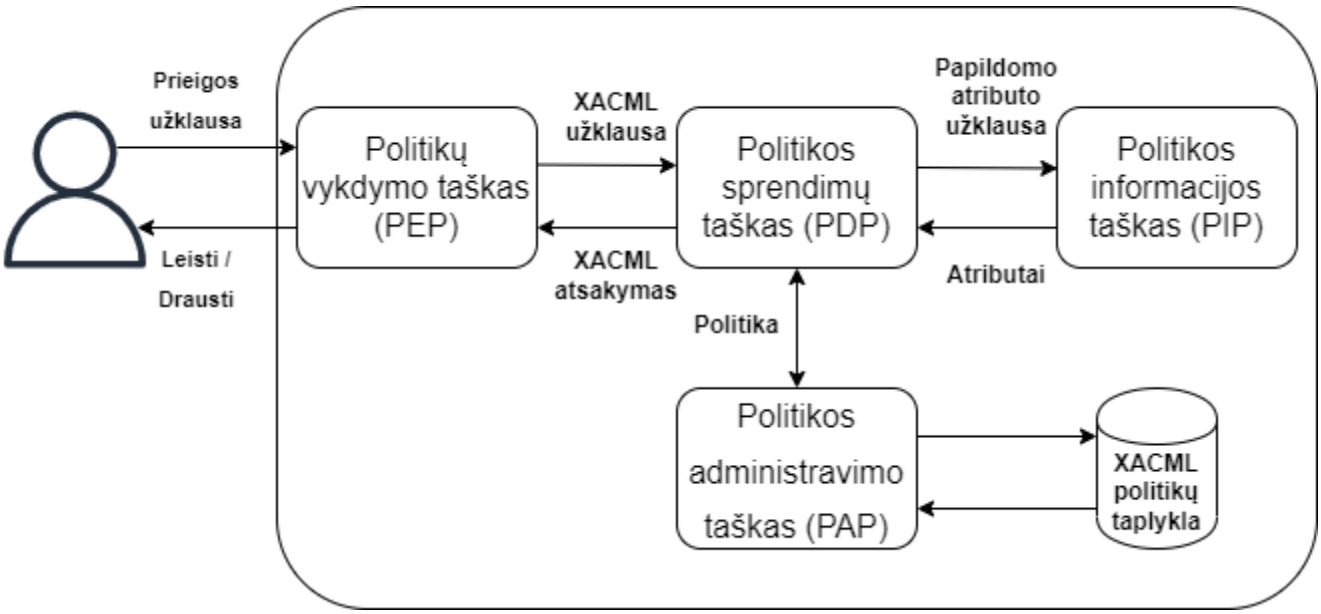
- SecureTrack – tinklo saugos valdymo sprendimas, kuris užtikrina tinklo saugos politikos matomumą, valdymą ir stebėjimą. Tai padeda organizacijoms analizuoti politiką, sekti pokyčius, stebėti tinklo srautą realiuoju metu, užtikrinti atitiktį ir kurti ataskaitas;
- SecureChange – saugos automatizavimo sprendimas, kuris supaprastina ir automatizuoja tinklo saugos politikos pakeitimų įgyvendinimo procesą. Sprendimas įgyvendina darbo eigos automatizavimą, rizikos analizę, integravimą su tinklo įrenginiais.
- SecureApp – sprendimas, leidžiantis organizacijoms tvarkyti ir stebėti įvairių programų generuojamą tinklo srautą;
- SecureCloud – tinklo saugos debesijos ir hibridinės debesijos aplinkos valdymo sprendimas, padedantis valdyti tinklo saugos politiką ir atitiktį debesijos platformose.

1.8. Saugos politikos automatizuoto valdymo modeliai

Šiame skyrelyje yra apžvelgti egzistuojantys, literatūroje ir straipsniuose pasiūlyti saugumo politikų automatizuoto valdymo modeliai.

1.8.1. XACML prieigos kontrolės politikų valdymo modelis

XACML yra XML paremta kalba, skirta apibrėžti ir vykdyti prieigos kontrolės politiką. XACML suteikia galimybę trečiųjų šalių programoms / komponentams vykdyti atributais pagrįstą prieigos valdymą (angl. *Attribute-based Access Control*). XACML leidžia administratoriams apibrėžti prieigos prie išteklių taisykles, pagrįstas įvairiais atributais, tokiais kaip vartotojo tapatybė, vaidmuo, vieta, paros laikas ir ištekliaus svarbos lygis. XACML modelis pavaizduotas 1.17 pav.



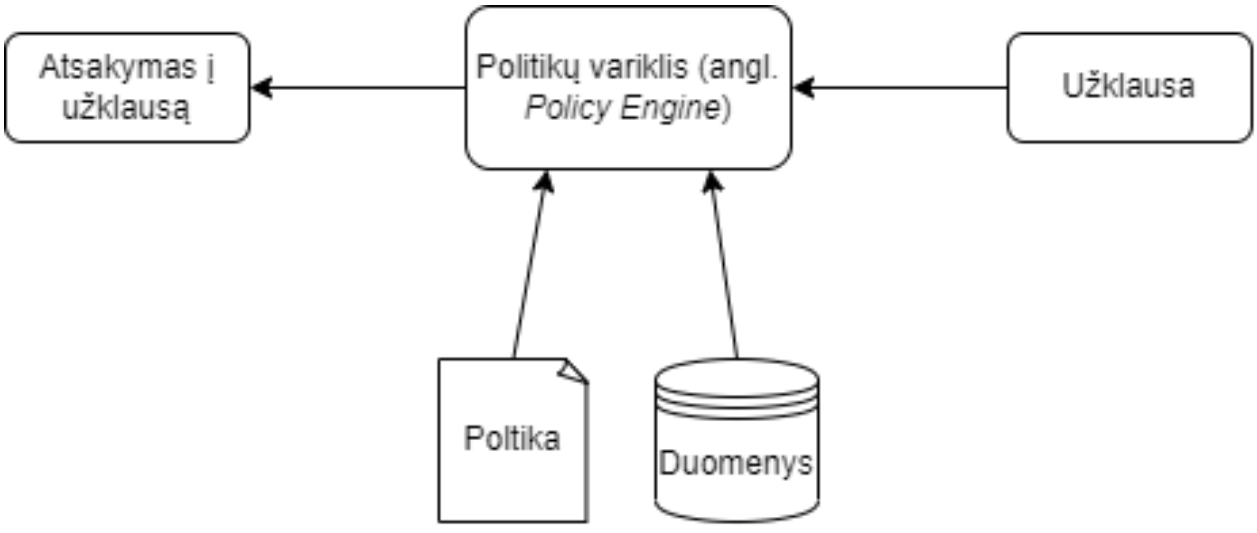
1.17 pav. XACML modelis

Modelis sudarytas iš šių komponentų [21]:

- PEP (angl. *Policy Enforcement Point*) – komponentas, perimantis prieigos užklausą ir priimantis sprendimą apie tai patvirtinti ar atmesti prieigos užklausą. PEP siunčia PDP prašymą priimti sprendimą dėl prieigos ir vykdo PDP grąžintą sprendimą;
- PDP (angl. *Policy Decision Point*) – komponentas, priimantis prieigos užklausą ir grąžinantis sprendimą PEP dėl prieigos prie ištekliaus. PDP gauna prieigos užklausas iš PEP ir įvertina užklausą pagal PIP apibrėžtas politikos taisykles;
- PIP (angl. *Policy Information Point*) – komponentas, į kurį PDP gali kreiptis ir gauti daugiau informacijos, kurios reikia, kad būtų priimtas sprendimas dėl prieigos. Pavyzdžiui, jei PDP gauna vartotojo vardą kaip atributą, jis gali kreiptis į PIP ir gauti tam vartotojui priskirtų vaidmenų rinkinį, kad priimtų sprendimą dėl to ar suteikti, ar uždrausti prieigą prie šaltinio;
- PAP (angl. *Policy Administration Point*) – komponentas, valdantis politiką ir taisykles, kurias PDP naudoja sprendimams dėl prieigos priimti. PAP yra atsakingas už politikos kūrimą, atnaujinimą ir ištrynimą;
- XACML politikų talpykla – prieigos politikų saugykla. PAP naudoja politikų saugyklą politikoms saugoti, kurti, atnaujinti ir trinti. PAP saugo politikas saugykloje, kad PDP galėtų lengvai jas pasiekti politikos taikymo metu.

1.8.2. *Policy as code* modelis

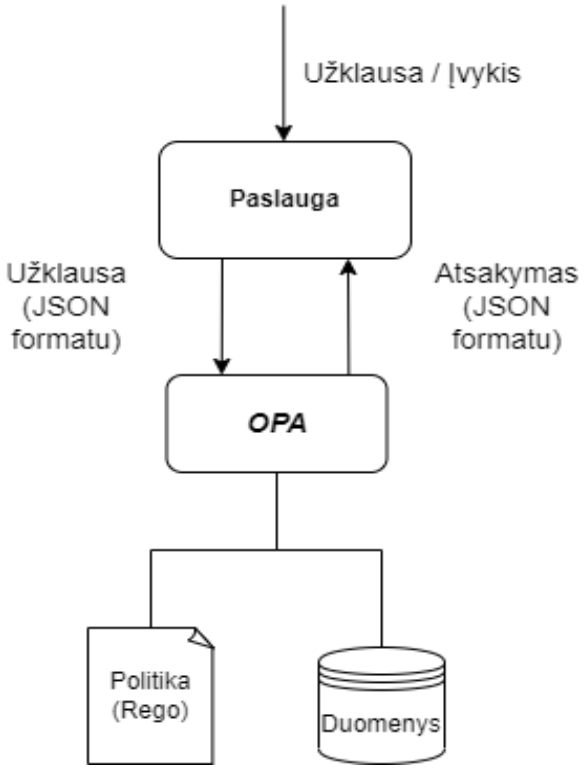
Politikos kaip kodo (angl. *Policy as code*) modelis yra politikos automatizavimo sprendimas, kuris įgyvendinamas naudojant aukšto lygio programavimo kalbą. Aukšto lygio programavimo kalba sąveikauja su politikų varikliu (angl. *Policy Engine*), kuriam reikalinga įvestis, duomenys ir politika, kad būtų sugeneruotas užklausos rezultatas. Taikant šį modelį, politikų taisyklės realizuojamos naudojant programavimo kalbą, kurios pagalba politikos taisyklės įgyvendinimas arba atitikties tikrinimas išreiškiami programinių veiksmų seka. Modelis yra pavaizduotas 1.18 pav.



1.18 pav. *Policy as code* modelis

1.8.3. Open Policy Agent

Open Policy Agent (OPA) yra atvirojo kodo įrankis, įgyvendinantis *Policy as code* koncepciją ir politikomis grįstą kontrolę, bet kokio tipo infrastruktūrai padedančią pagreitinti politikos ir taisyklių tikrinimo procesą, įvertinant infrastruktūros kodą prieš jam patenkant į produkcinę aplinką. Pavyzdžiui įrankis puikiai pritaikomas priešdiegiminėje stadijoje, kuomet pirmiausia patikrinama politikų bei taisyklių atitiktis, o tik tada siunčiama diegimo komanda į konkrečią infrastruktūrą. Saugumo politikos yra realizuojamos Rego programavimo kalba. OPA modelis yra pavaizduotas 1.19 pav.



1.19 pav. OPA veikimo schema

OPA gali būti pritaikytas Kubernetes, Docker, Elastic, Terraform, Kafka, Ceph ir panašaus pobūdžio technologijose [23].

1.9. Išvados

Skyriuje apžvelgti saugumo politikos apibrėžimai, svarbiausi informacinės saugos aspektai bei iššūkiai, su kuriais susiduria organizacijos valdydamos prieigą prie informacinių išteklių. Taip pat pristatyti egzistuojantys IT saugos politikos automatizuoto valdymo modeliai. Apibendrinus atliktą analizę galima padaryti kelias išvadas:

1. Saugos politika yra neatsiejama informacinės saugos grandinės dalis.
2. Sėkmingas saugos politikos sukūrimas ir pritaikymas organizacijoje yra didelių pastangų reikalaujanti užduotis, kadangi dalis žmonių yra vis dar linkę manyti, kad tam tikrų saugumo politikų laikymasis yra nereikalingas ir daug laiko atimantis procesas.
3. SANS saugumo politikų šablonai yra vienas iš pasirinkimų pradedant plėtoti organizacijos saugos politiką.
4. Išanalizavus egzistuojančius saugos politikos automatizuoto valdymo modelius pastebėta, kad jie veikia įvestis – vykdymas – išvestis principu.
5. Egzistuojantys saugos politikos automatizuoto valdymo modeliai yra panašūs savo struktūra, kadangi yra sudaryti iš panašią paskirtį turinčių elementų kaip saugumo politikų talpykla, politikų apdorojimo komponentas.
6. Politikos atitikties patikra ir užtikrinimas visų pristatytų modelių atveju yra išverčiami į programines veiksmų sekas.

2. IT SAUGOS POLITIKOS AUTOMATIZUOTO VALDYMO SISTEMOS MODELIS

2.1. Tikslas

Modelio tikslas yra automatizuoti saugumo politikų valdymą siekiant apsaugoti organizacijos infrastruktūrą nuo klaidingai sukonfigūruotų, saugumo politikų neatitinkančių įrenginių bei palengvinti jų konfigūravimo procesą. Tikslo įgyvendinimui keliami šie uždaviniai:

- Aprašyti tikslinės organizacijos infrastruktūrą, kurioje atsispindėtų organizacijos tinklas ir jos įrenginiai;
- Pasiūlyti ir aprašyti politikos struktūrą kompiuteriui suprantamu formatu (JSON, XML, YAML, XACML ar kitais formatais);
- Aprašyti tekstinės žemo lygio saugumo politikos išvertimo į kompiuterizuotą saugumo politiką procesą;
- Aprašyti kompiuterizuotos saugumo politikos atitikties tikrinimo procesą;
- Aprašyti aptiktų kompiuterizuotos saugumo politikos pažeidimų šalinimo (užtikrinimo) procesą;
- Aprašyti naujo įrenginio sukonfigūravimo pagal pasiūlytą kompiuterizuotą saugumo politiką procesą.

2.2. Esamos situacijos analizė

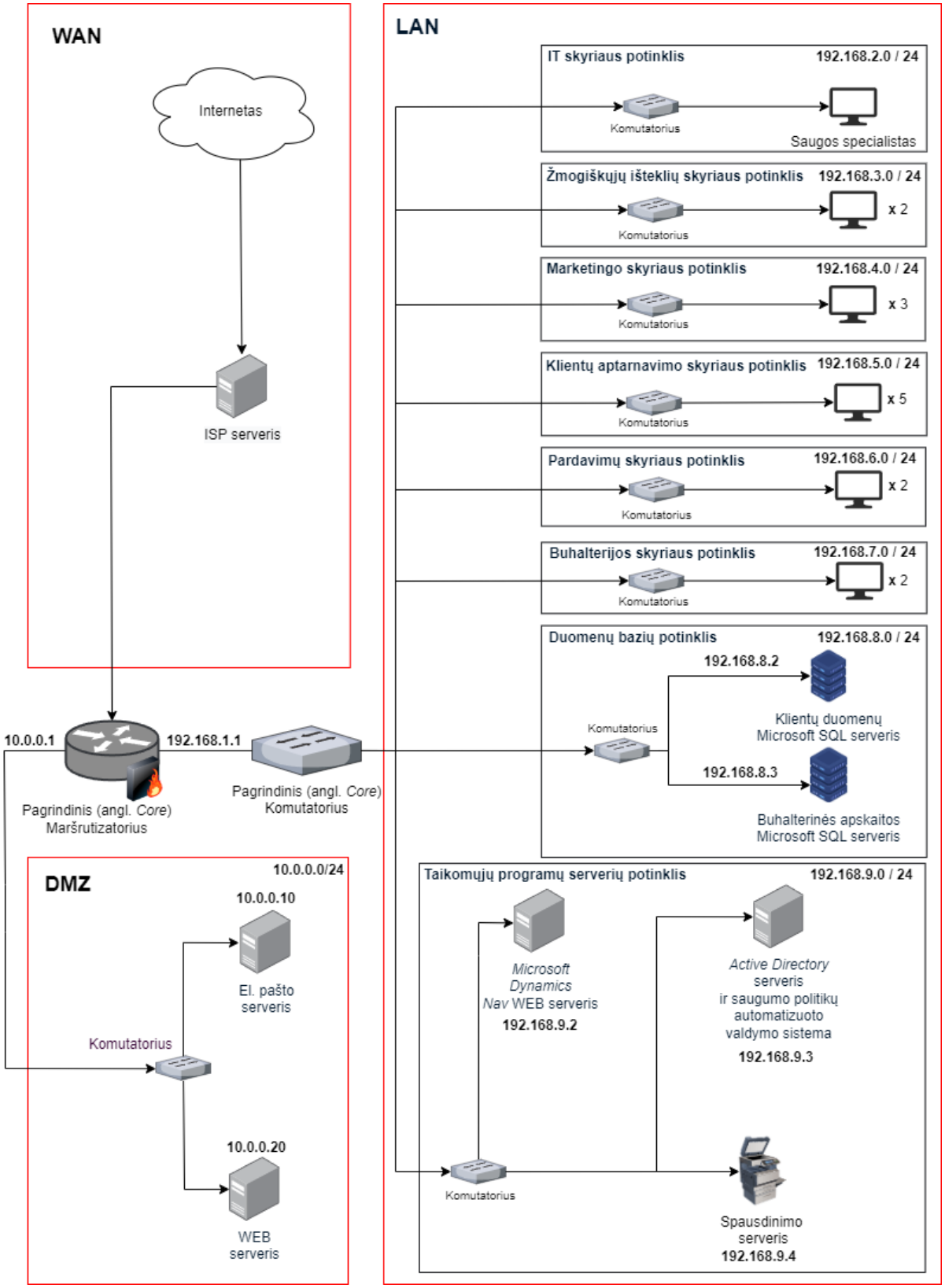
2.1 pav. yra pavaizduota tikslinės organizacijos tinklo infrastruktūra. Tinklo infrastruktūros schema yra suskaidyta į tris dalis: WAN (angl. *Wide Area Network*), DMZ (angl. *Demilitarized zone*) bei LAN (angl. *Local Area Network*). Vienas svarbiausių organizacijos tinklo elementų yra pagrindinis maršrutizatorius, jungiantis šias tris tinklo dalis. DMZ zona apima viešai prieinamas paslaugas, į kurias įeina: elektroninio pašto serveris ir WEB serveris. Vidinė organizacijos tinklo dalis yra suskirstyta į 8 potinklius:

- IT skyriaus potinklis (192.168.2.0/24);
- Žmogiškųjų išteklių skyriaus potinklis (192.168.3.0/24);
- Marketingo skyriaus potinklis (192.168.4.0/24);
- Klientų aptarnavimo skyriaus potinklis (192.168.5.0/24);
- Pardavimų skyriaus potinklis (192.168.6.0/24);
- Buhalterijos skyriaus potinklis (192.168.7.0/24);
- Duomenų bazių potinklis (192.168.8.0/24);
- Taikomųjų programų potinklis (192.168.9.0/24).

Šiems potinkliams priklauso darbiniai kompiuteriai, spausdintuvai ir kiti organizacijos tinklo įrenginiai. Duomenų bazių potinkliui priklauso dvi – klientų bei apskaitos duomenų saugyklos. Kai kurie skyriai naudoja tam tikrą programinę įrangą, kurios serveriai yra taikomųjų programų serverių potinklyje. Organizacijos darbuotojų naudojamos taikomosios programos (jų serveriai):

- Microsoft Dynamics Nav Web serveris – apskaitos vedimo tikslams naudojama programinė įranga;
- Active Directory serveris – kompiuterių ir vartotojų saugumo politikų valdymo serveris naudojamas organizacijos domeno valdymui;

- Spausdinimo serveris – visiems organizacijos vidinio tinklo potinklių vartotojams skirtas spausdintuvas.

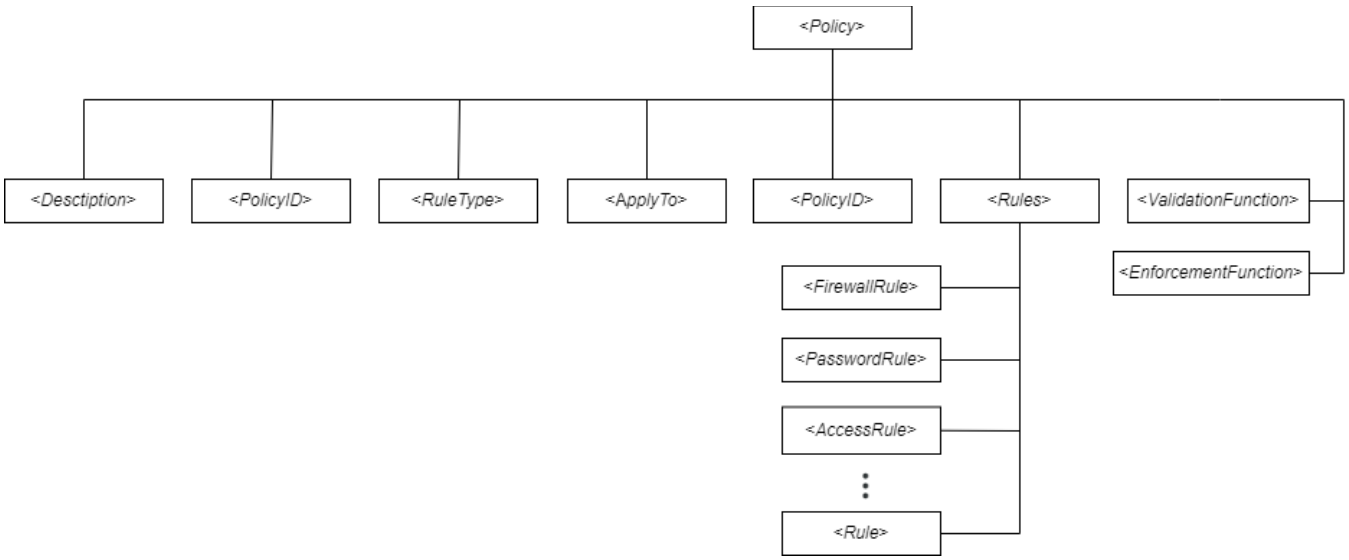


2.1 pav. Organizacijos tinklo infrastruktūros schema

2.3. Kompiuterizuota saugumo politika ir sistemos modelis

2.3.1. Kompiuterizuotos saugumo politikos struktūra

Tekstinė žemo lygio saugumo politika yra išverčiama į XML tipo kompiuterizuotą saugumo politiką (toliau - KSP). Žemiau esančiame 2.2 pav. pavaizduota XML saugumo politikos objekto struktūra.



2.2 pav. XML saugumo politikos struktūra

KSP sudaro 8 privalomi atributai:

- **Description** – tekstinės žemo lygio saugumo politikos aprašymas;
- **PolicyID** – KSP identifikacinis numeris;
- **RuleType** – atributas, nusakantis kokio tipo taisykles realizuoja KSP;
- **ApplyTo** – atributas, nusakantis kam – kokiam įrenginiui ar jų grupei politika yra taikoma;
- **PolicyID** – KSP identifikatorius;
- **Rules** – *RuleType* atribute nurodytos reikšmės tipo taisyklių sąrašas;
- **ValidationFunction** – programinė funkcija, tikrinanti kiekvienos taisyklės atitiktį;
- **EnforcementFunction** – programinė funkcija, atliekanti saugumo politikos atitikties užtikrinimą.

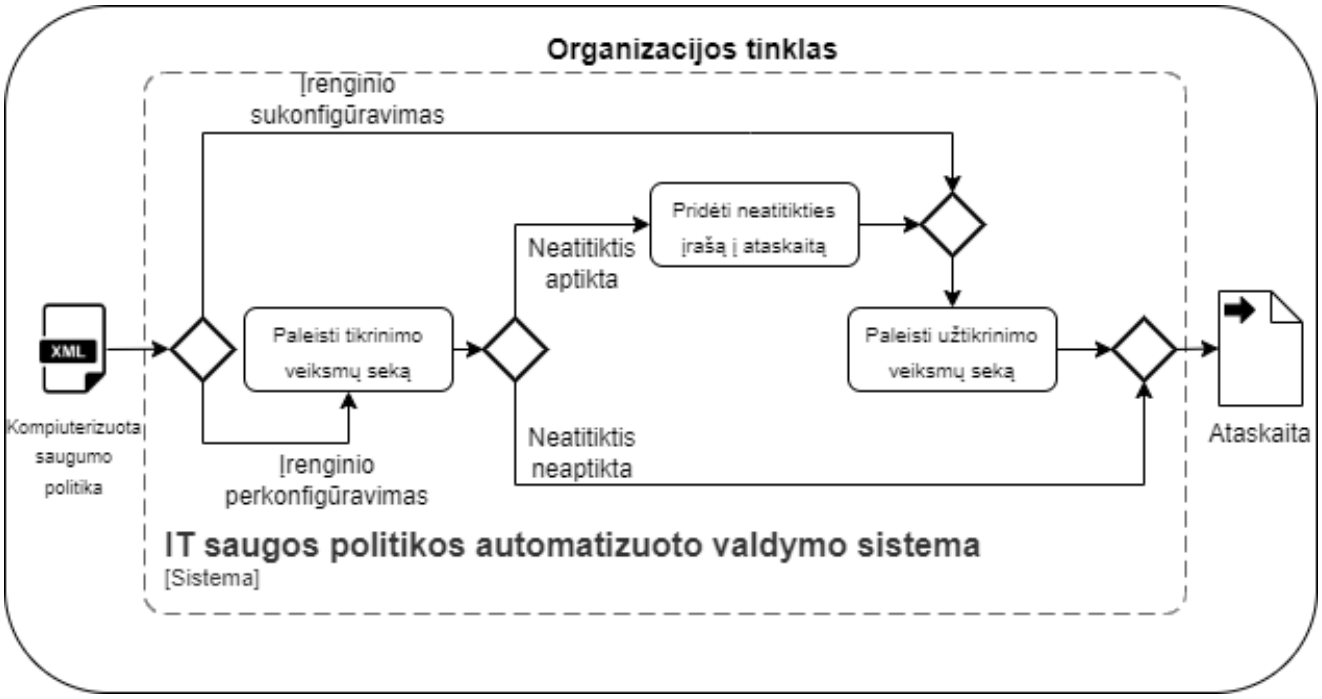
Viena KSP gali realizuoti neribotą skaičių taisyklių su sąlyga, kad visos jos privalo būti vieno ir to pačio tipo. Jeigu žemo lygio saugumo politikos neįmanoma realizuoti naudojant vieno tipo KSP taisyklę, rekomenduojama sukurti atskirą KSP, realizuojančią trūkstamus žemos saugumo politikos punktus. KSP atitikties valdymo automatizavimui naudojamos tam tikros nuo taisyklės tipo priklausančios programinės funkcijos (*ValidationFunction* bei *EnforcementFunction*), kurios patikrina bei esant poreikiui atlieka reikiamus pakeitimus taisyklių realizacijoje. Šioje vietoje yra vienintelė sąlyga - funkcijos turi priimti įvesties parametrus, atitinkančius taisyklės objekto atributų pavadinimus. Vėliau gali būti sugeneruojamos dviejų tipų komandos, kurios darbe vadinamos atitikties tikrinimo bei atitikties užtikrinimo veiksmų sekomis. Žemo lygio saugumo politikos kompiuterizavimo galimybė priklauso nuo sistemos su kuria siejama žemo lygio saugumo politika galimybių atlikti KSP taisyklių konfigūravimą programinės veiksmų sekos pagalba.

2.3.2. Sistemos modelis

Modelio funkcionalumą sudaro dvi pagrindinės funkcijos: įrenginio sukonfigūravimas ir perkonfigūravimas pagal saugumo politikas. Saugumo politikų automatizuoto valdymo sistemos modelis yra paremtas atviros sistemos modeliu, pasiūlytu dar šeštajame dešimtmetyje mokslininkų D. Katz ir R. L. Kahn, kurį sudaro aplinka, įvestis, procesas, išvestis bei grįžtamasis ryšys [24]. Sistema veikia su įrenginiais, kurie yra skirstomi į dvi kategorijas:

- Pirmą kartą konfigūruojami įrenginiai (sukonfigūruoti);
- Egzistuojantys įrenginiai, kurie kažkada buvo sukonfigūruoti, tačiau reikia atlikti įrenginio auditą ir patikrinti, ar įrenginio konfigūracija nebuvo pakeista (aptikus neatitiktį su KSP taisykle jį atitinkamai perkonfigūruoti).

2.3 pav. pavaizduotas sistemos modelis.



2.3 pav. Modelis

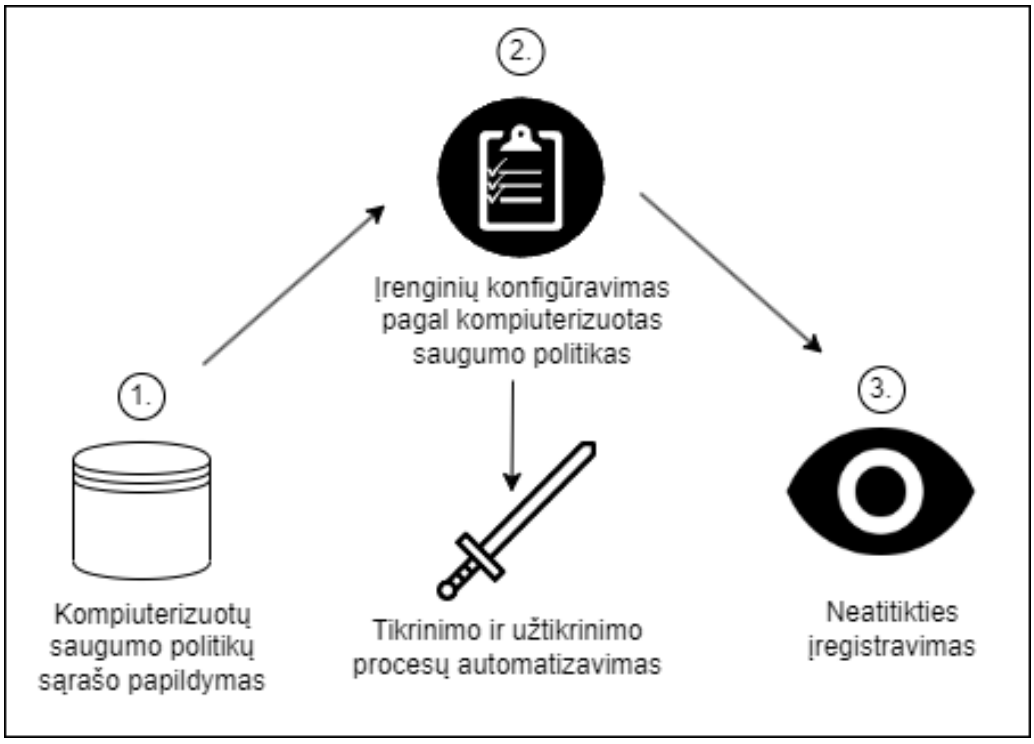
Sistema priima KSP kaip įvestį. Ji yra apdorojama nuskaitant jos atributų reikšmes. Auditorius paleisdamas sistemą pasirenka ar nori vykdyti įrenginio sukonfigūravimą pagal KSP, ar ieškoti KSP neatitikčių ir jų atradus vykdyti įrenginio perkonfigūravimą. Paleidus įrenginio sukonfigūravimą tikrinimo veiksmų seka nėra vykdoma, vykdoma tik užtikrinimo veiksmų seka, o tikrinant egzistuojančio įrenginio atitiktį leidžiama tikrinimo veiksmų seka ir priklausomai nuo to, ar paleidus tikrinimo veiksmų seką aptikta neatitikčių, ir užtikrinimo veiksmų seka. Naujai konfigūruojamo įrenginio atveju yra atliekama pilna įrenginio konfigūracija pagal KSP ir jos taisykles. Jos metu yra iteruojama per visą KSP sąrašą ir yra paleidžiamos kiekvienos KSP taisyklės atitikties užtikrinimo veiksmų seka. To rezultatas – saugiai sukonfigūruotas įrenginys, atitinkantis organizacijos KSP.

Jei pasirenkama opcija perkonfigūruoti įrenginį, kurio pirminė konfigūracija jau buvo atlikta anksčiau, organizacijos įrenginių atitikties patikros metu jame yra ieškoma neatitikčių (saugumo politikos pažeidimas). Aptikus pažeidimą įrenginys yra perkonfigūruojamas taip, kad atitiktų KSP ir

jos taisykles generuojant ir paleidžiant pažeistų KSP taisyklių užtikrinimo veiksmų sekas. To rezultatas – perkonfigūruotas įrenginys, atitinkantis organizacijos KSP. Pabaigus įrenginio perkonfigūravimą yra sugeneruojama ataskaita, kurioje atsispindi tikrinimo veiksmų sekų aptikti saugumo politikų pažeidimai. Taigi, apibendrinant galima teigti, kad pagrindinės modelio funkcijos yra:

- KSP sąrašo pildymas;
- Neatitikčių paieška;
- Įrenginio konfigūravimas pagal KSP;
- Neatitikčių įregistravimas.

Pagrindinės modelio funkcijos grafiškai pavaizduotos 2.4 pav.



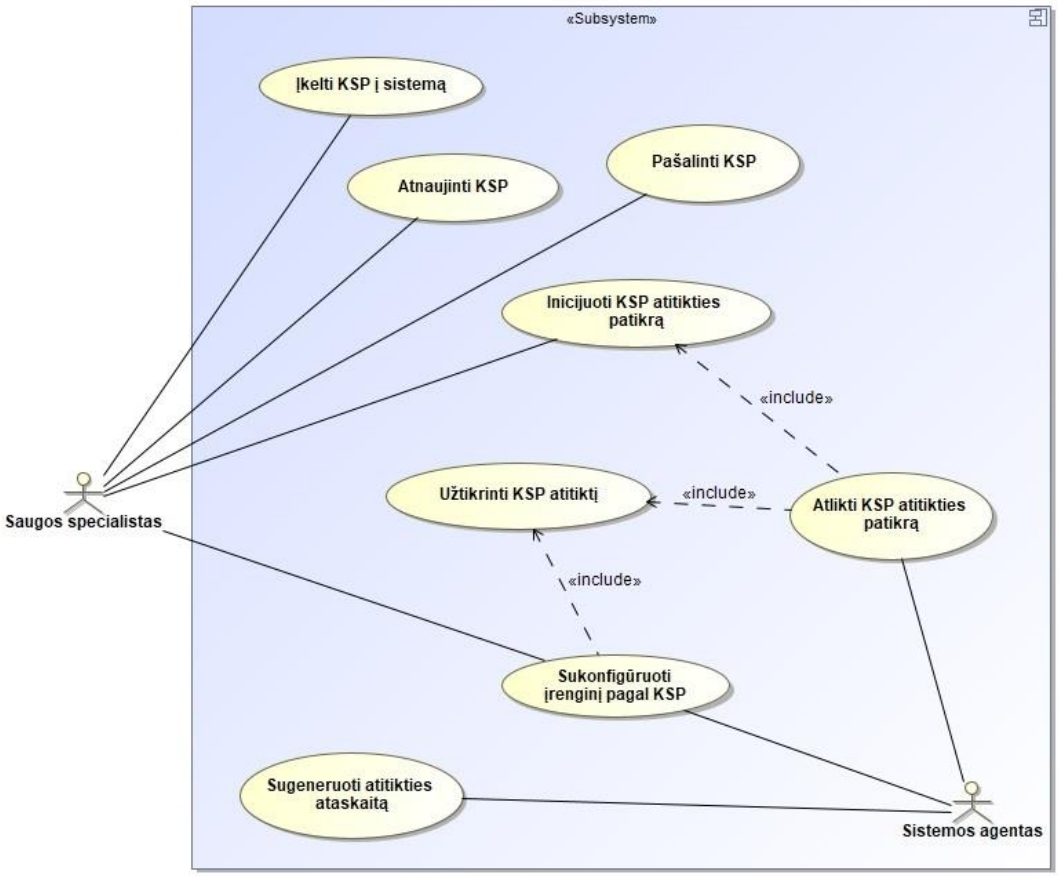
2.4 pav. Modelio funkcijos

2.4. Modelio reikalavimai

Modeliui yra keliami funkciniai ir nefunkciniai reikalavimai. Šiame skyrelyje pateikti abstraktūs modeliui keliami reikalavimai, kurie bus patikslinti modelio prototipo realizacijos dalyje.

2.4.1. Funkciniai reikalavimai

Modelis yra orientuotas į mažo bei vidutinio dydžio organizacijas, neturinčias didelio IT skyriaus. Funkciniai reikalavimai IT saugos politikos automatizuoto valdymo modeliui atvaizduoti panaudos atvejų diagramos pavidalu 2.5 pav.



2.5 pav. Modelio panaudos atvejų diagrama

2.4.2. Nefunkciniai reikalavimai

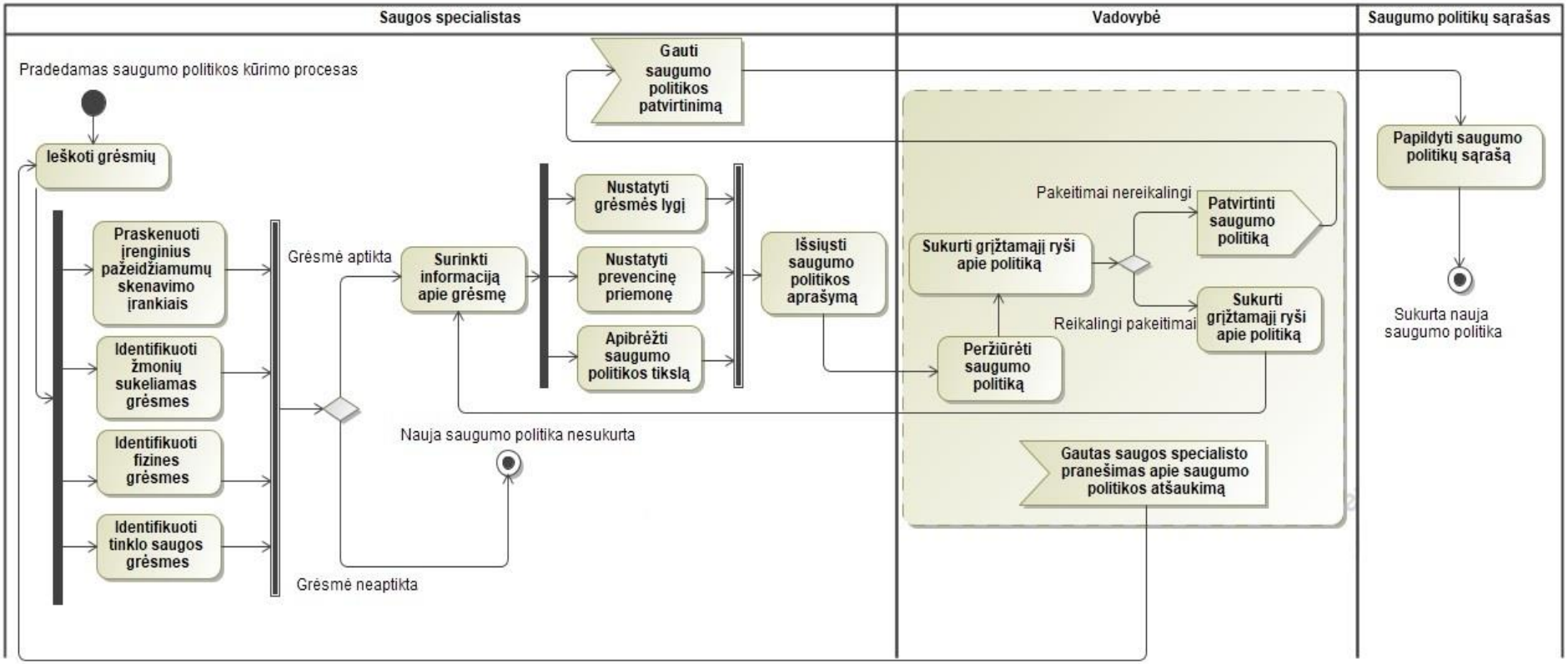
1. Sistema turi būti projektuojama taip, kad būtų pajėgi dirbti su dideliais KSP kiekiais;
2. Sistema turi turėti vartotojui draugišką sąsają;
3. Sistema turi būti projektuojama taip, kad ją būtų lengva pritaikyti naujų tipų saugumo politikoms.

2.5. Saugumo politikos kompiuterizavimas

Tekstinės žemo lygio saugumo politikos išvertimas į kompiuterizuotą yra rankiniu būdu, tačiau nesudėtingai atliekama užduotis.

2.5.1. Politikos kūrimo procesas

Saugumo politikų apibrėžimo procesas pradedamas grėsmių paieška, kurią atlieka organizacijos saugos specialistas. Jis atlikdamas programinės įrangos pažeidžiamumų skenavimus, stebėdamas darbuotojų saugos elgesio tendencijas, įžvelgdamas fizines grėsmes, stebėdamas organizacijos tinklo srautą identifikuoja įvairias galimas grėsmes. Remdamasis jomis paruošia žemo lygio saugumo politikos aprašymą, kurį vėliau siunčia vadovybei. Ji politiką arba patvirtina, arba atmeta reikalaudama atlikti tam tikrus pakeitimus. Galiausiai saugumo politika įtraukiama į organizacijos saugumo politikų sąrašą. 2.6 pav. pavaizduotas saugumo politikos įvedimo organizacijoje proceso UML modelis.



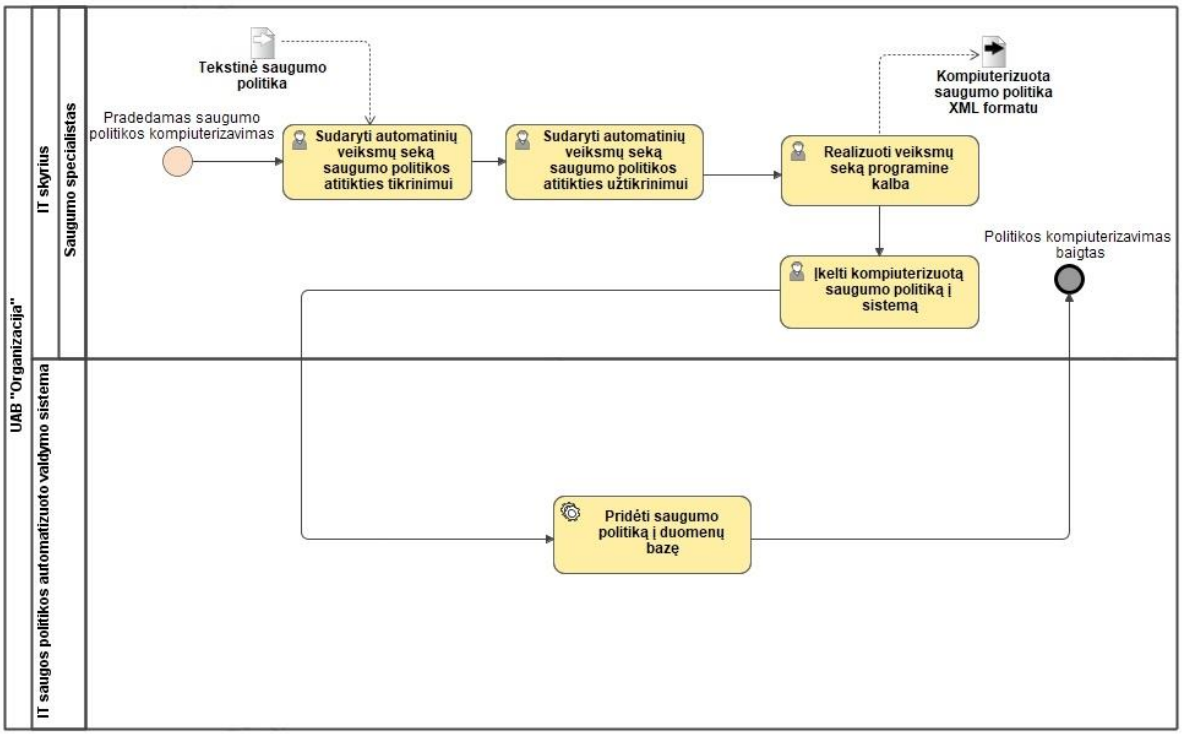
2.6 pav. Saugumo politikos įvedimo procesas

2.5.2. Politikos kompiuterizavimo procesas

Vadovybei patvirtinus žemo lygio saugumo politiką galima pradėti jos kompiuterizavimą. Yra du pagrindiniai šį procesą apibūdinantys terminai:

- Žemo lygio saugumo politikos kompiuterizavimas – žemo lygio saugumo politikos išvertimo į kompiuteriui suprantamą formatą procesas;
- (Programinė) veiksmų seka – programavimo kalba realizuota veiksmų seka, kurios paskirtis yra atlikti KSP atitikties patikrą arba atitkties užtikrinimą.

2.7 pav. pavaizduotas žemo lygio saugumo politikos kompiuterizavimo procesas.



2.7 pav. Saugumo politikos kompiuterizavimo procesas

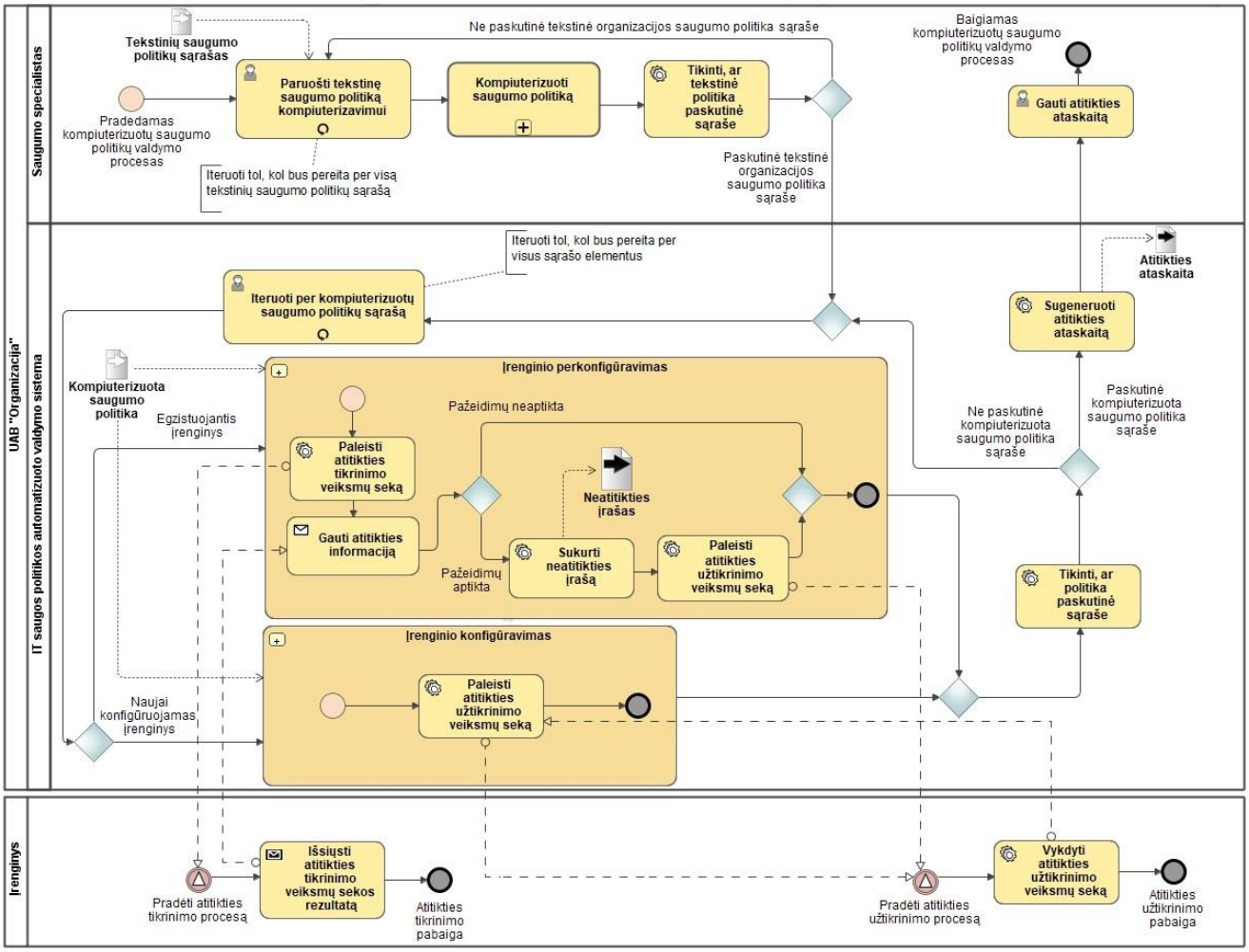
Saugos specialistas išanalizavęs žemo lygio saugumo politikos reikalavimus sukuria programinę veiksmų seką jos atitikties tikrinimui bei užtikrinimui. Pagal KSP struktūrą yra rankiniu būdu suformuojamas politikos XML objektas, kuris yra įkeliamas į sistemą.

2.6. Kompiuterizuotos saugumo politikos atitikties valdymas

Pagrindinis projektuojamos sistemos tikslas – valdyti KSP atitiktį. Valdyti kalbant apie šią sistemą reiškia tikrinti įrenginio atitiktį, aptikti politikų pažeidimus juos pašalinti paleidžiant programavimo kalba realizuotą veiksmų seką. Šio proceso metu saugos specialistas sąveikauja su sistema, o sistema sąveikauja įrenginiu įvairiais būdais priklausomai nuo audituojamo įrenginio ir galimybių su juo komunikuoti įskaitant, tačiau neapsiribojant:

- Išskirtu API, su kuriuo komunikuojant galima atlikti įrenginio konfigūravimą;
- Bash, PowerShell skriptais, galinčiais valdyti tūkstančius domeno įrenginių;
- Specifinių programinių įrangų CLI (angl. *Command Line Interface*) komandinėmis eilutėmis.

2.8 pav. pavaizduotas išsamus ir universalus KSP atitikties valdymo procesas, tinkantis įvairių tipų saugumo politikoms.



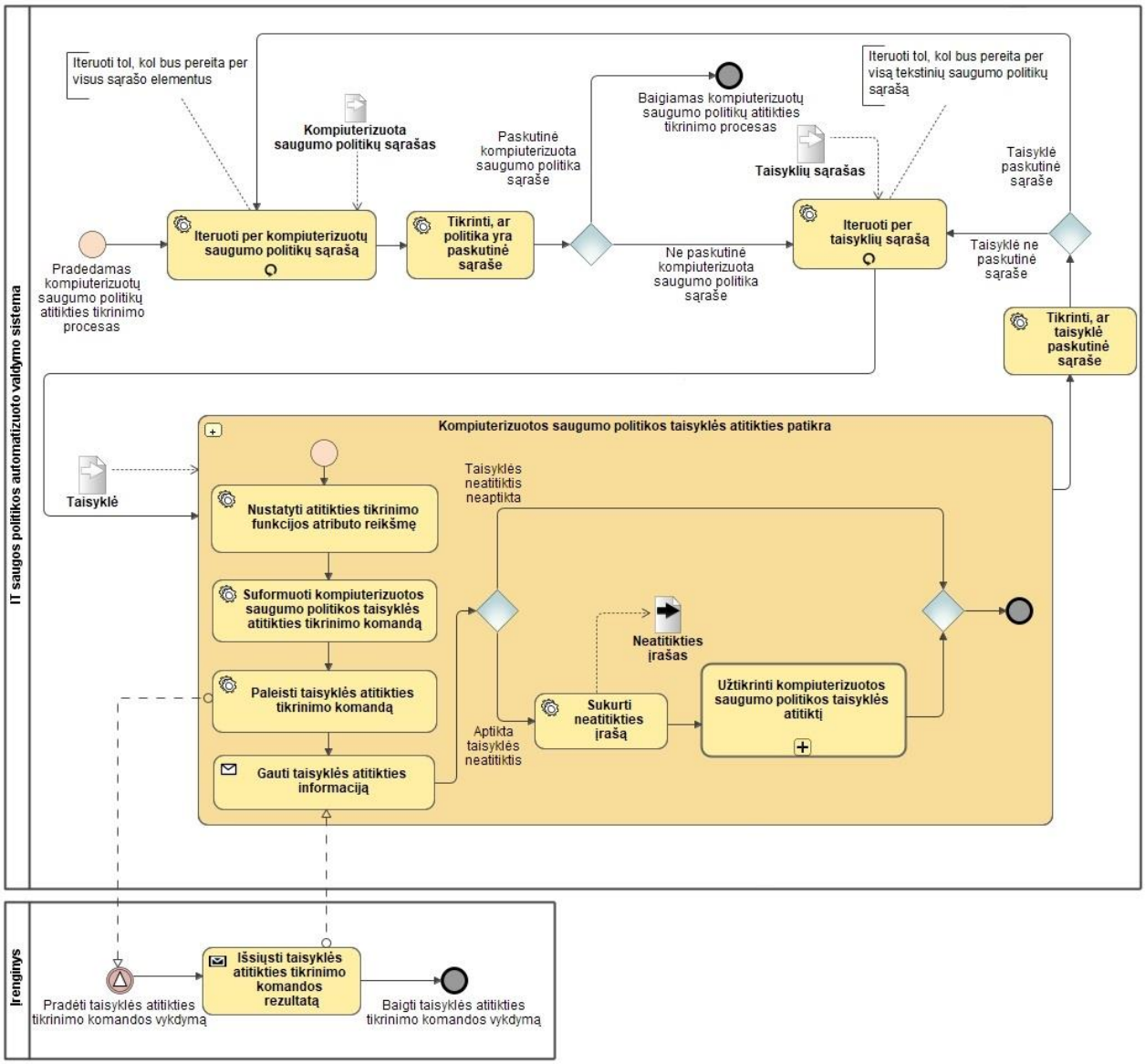
2.8 pav. Saugumo politikų valdymo procesas

Proceso pabaigoje sugeneruojama atitikties ataskaita, kurią proceso pabaigoje gali peržiūrėti saugos specialistas.

2.6.1. Kompiuterizuotos saugumo politikos atitikties tikrinimas

Tikrinimo metu yra iteruojama per KSP objektų sąrašą. Vienai po kitos yra atliekama atitikties patikra. KSP iš pradžių yra perduodama atitikties tikrinimo procesui. Proceso inicijavimui reikalingas KSP taisyklių sąrašas bei atitikties tikrinimo funkcijos pavadinimas. Toliau pradedamas iteravimas per KSP taisyklių sąrašą. Tikrinimo funkcijos įvestis – taisyklė, kurios atitiktis yra tikrinama įrenginyje. Jei KSP turi daugiau nei vieną taisyklę, baigus vienos taisyklės atitikties tikrinimą yra pereinama prie kitos taisyklės atitikties tikrinimo. Aptikus neatitiktį bent vienoje iš taisyklių yra sukuriamas neatitikties įrašas, kuris vėliau yra įtraukiamas į ataskaitą. Procesas kartojasi tol, kol bus pereita per visą KSP sąrašą. Galima teigti, kad KSP atitiktis yra lygi jos taisyklių atitikčiai. Bent vienoje iš taisyklių aptikus neatitikčių yra laikoma, kad įrenginys neatitinka KSP. Sistemai aptikus politikos pažeidimą yra iškviečiamas kitas veiklos procesas pavadinimu „Užtikrinti atitiktį“, jo tikslas – paversti įrenginį iš „nesilaikančio saugumo politikos“ statuso į

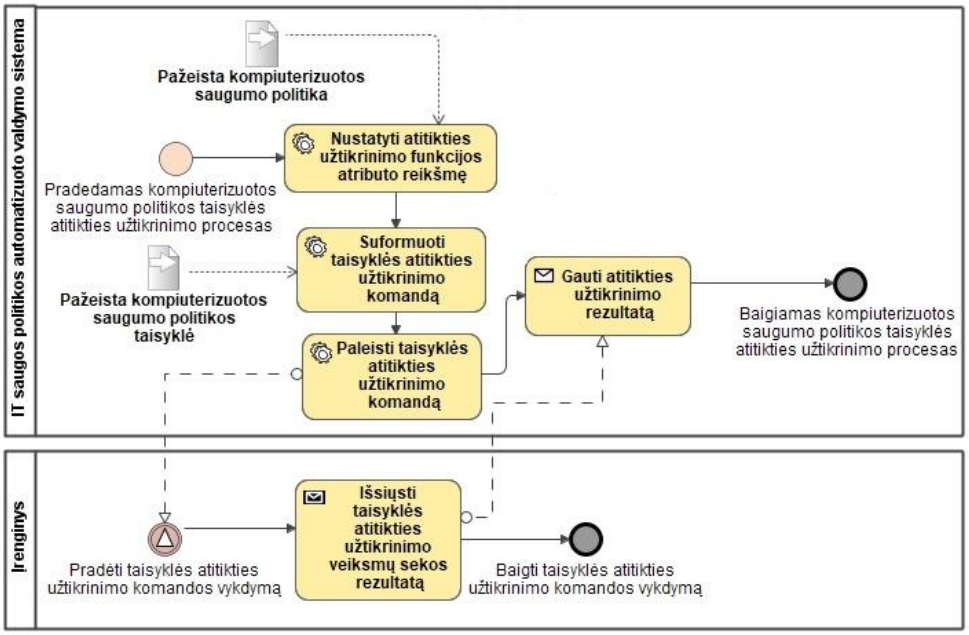
„besilaikantį saugumo politikos“ arba kitaip tariant – procesas pašalinantis saugumo politikos pažeidimą įvykdant atitikties užtikrinimo veiksmų seką. Proceso pabaigoje sugeneruojama atitikties ataskaita. 2.9 pav. pavaizduotas KSP atitikties tikrinimo procesas.



2.9 pav. Tikrinti kompiuterizuotos saugumo politikos atitiktį

2.6.2. Kompiuterizuotos saugumo politikos taisyklės atitikties užtikrinimas

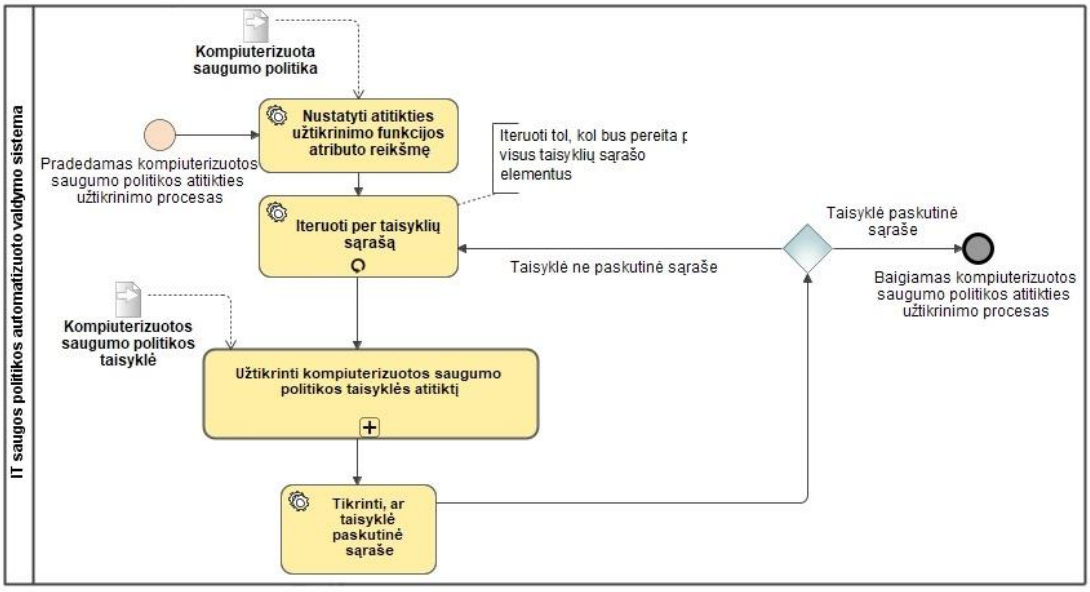
Tikrinimo proceso metu aptikus, kad įrenginys neatitinka vienos ar daugiau taisyklių, inicijuojamas taisyklės atitikties užtikrinimo procesas. Šio proceso tikslas yra perkonfigūruoti įrenginį taip, kad po perkonfigūravimo įrenginys atitiktų prieš tai pažeistą KSP taisyklę. Procesui perduodami parametrai – taisyklė bei atitikties užtikrinimo funkcijos pavadinimas. Proceso vykdymo rezultatas apie tai, ar pavyko užtikrinti taisyklės atitiktį, atsispindi galutinėje atitikties ataskaitoje. 2.10 pav. pavaizduotas KSP taisyklės atitikties užtikrinimo procesas.



2.10 pav. Užtikrinti kompiuterizuotos saugumo politikos taisyklės atitiktį

2.6.3. Kompiuterizuotos saugumo politikos atitikties užtikrinimas

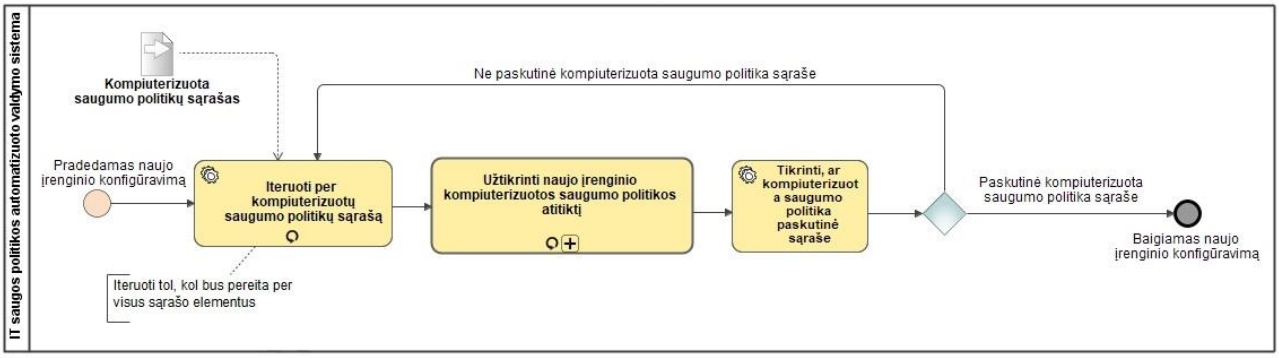
Proceso inicijavimui reikalinga KSP bei joje nurodytas taisyklių atitikties užtikrinimo funkcijos pavadinimas. Proceso metu yra iteruojama per KSP sąrašą ir kiekvienai KSP taisyklei yra sugeneruojama ir paleidžiama individuali programinė užtikrinimo veiksmų seka. Ji niekuo nesiskiria nuo tos, kuri yra paleidžiama aptikus taisyklės neatitiktį. Svarbu paminėti, kad konfigūruojant naują įrenginį KSP taisyklių atitiktis nėra tikrinama, iškart yra einama prie jų užtikrinimo (sukonfigūravimo) įrenginyje. 2.11 pav. pavaizduotas KSP taisyklės atitikties užtikrinimo procesas.



2.11 pav. Užtikrinti kompiuterizuotos saugumo politikos atitiktį

2.6.4. Naujo įrenginio konfigūravimas

Šio proceso metu vyksta naujo įrenginio sukonfigūravimas pagal organizacijos KSP. Procesas kaip įvestį gauna KSP sąrašą. Proceso metu yra iteruojama per KSP sąrašą ir užtikrinama kiekvienos sąraše esančios taisyklės atitiktis. 2.12 pav. pavaizduotas KSP taisyklės atitikties užtikrinimo procesas.



2.12 pav. Sukonfigūruoti įrenginį pagal kompiuterizuotą saugumo politiką

2.7. Išvados

Sukūrus IT saugos politikos automatizuoto valdymo modelį ir viską apibendrinus galima padaryti šias išvadas:

1. Saugos specialistas sistemą naudoja įrenginių atitikties patikrai su tikslu įrenginyje identifikuoti saugumo politikų pažeidimus arba sukonfigūruoti įrenginį pagal kompiuterizuotą saugumo politiką.
2. Pasiūlyta kompiuterizuotos saugumo politikos struktūra ir modelis gali būti pritaikomas įvairių tipų saugumo politikoms ir aplinkoms.
3. Žemo lygio saugumo politikos kompiuterizavimas yra atliekamas rankiniu būdu, tačiau tai nėra sudėtingas ir daug laiko užimantis procesas.
4. Automatinis atitikties valdymas gerokai sumažina žmogiškųjų pastangų poreikį bei laiko sąnaudas atliekant auditus.

3. IT SAUGOS POLITIKOS AUTOMATIZUOTO VALDYMO MODELIO PROTOTIPO ĮGYVENDINIMAS

Antrajame skyriuje aprašytas IT saugos politikos automatizuoto valdymo modelio prototipas bus įgyvendinamas automatizuojant atitikties valdymą Active Directory aplinkoje valdant grupės politikas (toliau - GP) bei jų pagalba konfigūruojamų registrų, Windows Defender ugniasienės tinklo profilių bei tinklo srauto taisyklių atitiktį. Sistemos plėtojimui bus naudojamos *GroupPolicy* ir *NetSecurity* PowerShell moduliuose aprašytos funkcijos.

3.1. Funkciniai reikalavimai

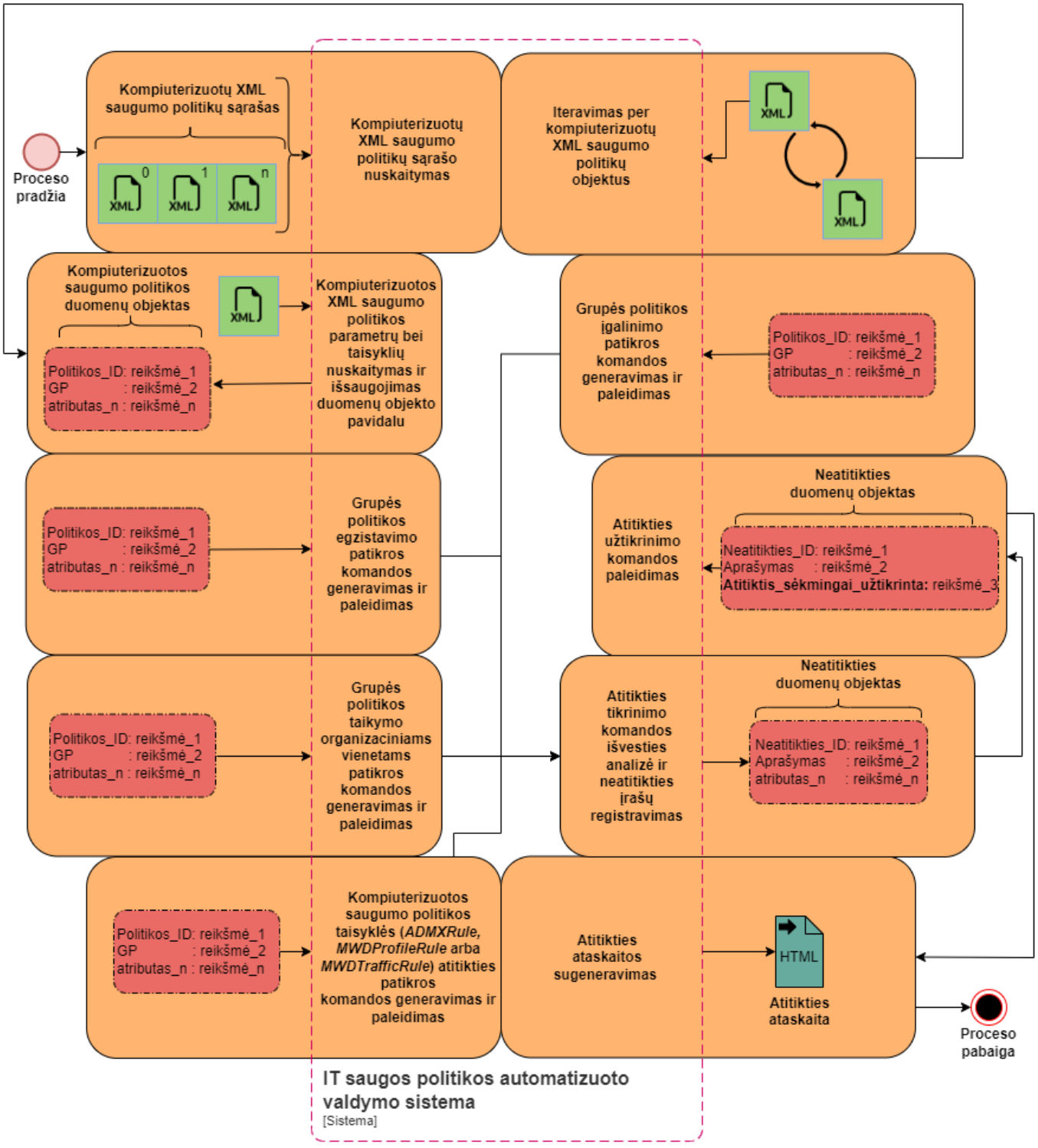
1. Sistemos realizacijai naudojama Windows Server 2019 operacinė sistema ir PowerShell skriptavimo kalba;
2. Sistema veikia lokaliame Active Directory serveryje;
3. Sistema turi būti įgyvendinta terminalinėje vartotojo sąsajoje;
4. Sistema turi kaip įvestį priimti XML formatu aprašytą KSP;
5. Sistema turi iteruoti per KSP sąrašą ir kiekvieną KSP apdoroti kaip įvestį;
6. Sistema turi gebėti konfigūruoti Active Directory GP pagal KSP tiek nuo pradžių, tiek patikrinti jau egzistuojančią konfigūraciją;
7. KSP taisyklės atitiktis turi būti tikrinama sugeneruojant ir paleidžiant PowerShell atitikties tikrinimo komandą;
8. KSP taisyklės atitiktis turi būti užtikrinta sugeneruojant ir paleidžiant PowerShell atitikties užtikrinimo komandą;
9. Konfigūruojant Active Directory GP nuo pradžių, turi būti leidžiamos tik atitikties užtikrinimo PowerShell komandos;
10. Aptiktos neatitiktys ir jų užtikrinimo rezultatai turi būti išsaugoti PowerShell duomenų struktūrų objektuose;
11. Patikrinus visų KSP atitiktį HTML formatu turi būti sugeneruojama atitikties ataskaita.

3.2. Nefunkciniai reikalavimai

1. Sistema turi gebėti valdyti didelius kiekius KSP ir užtikrinti augančius organizacijos saugumo poreikius;
2. Sistemos programinis kodas turi būti aiškus, kad ateityje būtų lengva jį suprasti ir esant poreikiui atnaujinti;
3. Sistema turi būti lengvai išplečiama, kad esant poreikiui būtų galima įgyvendinti kitų tipų saugumo politikų atitikties valdymo automatizavimą.

3.3. Modelis

Programos kodas ir testiniai duomenys yra talpinami sisteminiame aplanke pavadinimu „Prototipas“. Šio aplanko viduje yra prototipo programinio kodo failas pavadinimu „Prototipas.ps1“ ir aplankas „Politikos“, kuriame talpinami kompiuterizuotų saugumo politikų XML failai. Atitikties ataskaitos išsaugomos yra išsaugomos tame pačiame aplanke, kur ir leidžiamas prototipo programinis kodas. Sistemos modelis vizualiai pavaizduotas 3.1 pav.



3.1 pav. Modelis

Programos veikimas išskiriamas į 11 žingsnių:

1. KSP sąrašo nuskaitymas;
2. Iteravimas per KSP sąrašą;
3. KSP konvertavimas į PowerShell duomenų objektą;
4. Atitikties patikrai reikalingų duomenų objekto atributų nuskaitymas;
5. Atitikties patikros PowerShell komandos sugeneravimas;
6. Atitikties patikros PowerShell komandos paleidimas;
7. Atitikties patikros PowerShell komandos išvesties analizė;
8. Atitikties užtikrinimo PowerShell komandos sugeneravimas;
9. Atitikties užtikrinimo PowerShell komandos paleidimas;
10. Neatitikties įrašo (objekto) sukūrimas;
11. Atitikties ataskaitos sugeneravimas.

Programiniu būdu įgyvendinus šiuos žingsnius, sistema visapusiškai užtikrina sistemai perduotų KSP atitiktį.

3.4. Kompiuterizuota saugumo politika

Kompiuterizuota saugumo politika yra realizuota XML formatu bei paremta 2.3.1 skyrelio aprašu.

3.4.1. Struktūra

3.2 pav. pavaizduota KSP struktūra XSD formatu.

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
    xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <xs:element name="Policy">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="Description" type="xs:string" />
                <xs:element name="PolicyID" type="xs:string" />
                <xs:element name="PolicyType" type="xs:string" />
                <xs:element name="GroupPolicyName" type="xs:string" />
                <xs:element name="ApplyTo">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element maxOccurs="unbounded"
                            name="DistinguishedName" type="xs:string" />
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
                <xs:element name="Rules">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element maxOccurs="unbounded" name="Rule" />
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
                <xs:element name="ValidationFunction" type="xs:string" />
                <xs:element name="EnforcementFunction" type="xs:string" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>
</xs:schema>
```

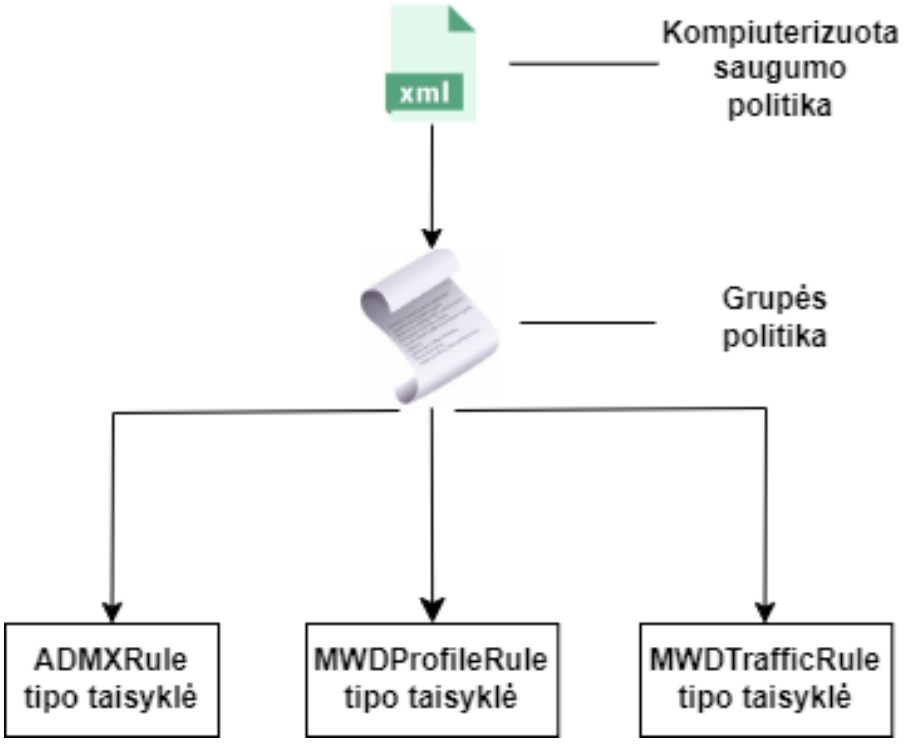
3.2 pav. Kompiuterizuotos saugumo politikos XML objekto struktūra

KSP yra sudaryta iš 9 atributų:

- **Description** – žemo lygio saugumo politikos aprašymas;
- **PolicyID** – KSP unikalus identifikacinis numeris;
- **RuleType** – KSP taisyklių tipas;
- **GroupPolicyName** – GP pavadinimas;
- **DistinguishedName** – organizacinio vieneto (toliau – OV), kuriam taikoma KSP, pavadinimas;
- **ApplyTo** – *DistinguishedName* tipo reikšmių sąrašas;
- **Rules** – KSP taisyklių sąrašas. Sąraše gali būti talpinamos tik *RuleType* atribute nurodyto tipo taisyklės;
- **ValidationFunction** – funkcija, atliekanti saugumo politikos atitikties patikrinimą;
- **EnforcementFunction** – funkcija, atliekanti saugumo politikos atitikties užtikrinimą.

3.4.2. Taisyklių tipai

Kiekviena KSP turi nuorodą į GP ir apibrėžia toje GP būtinai turinčias egzistuoti taisykles. KSP susideda iš vienos arba daugiau taisyklių todėl, kad siekiant išpildyti žemo lygio saugumo politikos reikalavimus ne visada pakanka sukurti vieną ugniasienės taisyklę arba pakeisti tik vieno registro rakto reikšmę. Teisingai įgyvendinus KSP aprašytas taisykles laikoma, kad KSP atitiktis yra užtikrinta. KSP loginė struktūra pavaizduota 3.3 pav.



3.3 pav. Kompiuterizuotos saugumo politikos loginė struktūra

Apibendrinus galima teigti, kad KSP yra platesnė organizacijos saugumo reikalavimo samprata, o taisyklė – konfigūracija, techniniai nustatymai, užtikrinantys KSP atitiktį. Kituose skyreliuose bus pristatyti KSP taisyklių tipai, kuriuos palaiko IT saugos politikos automatizuoto valdymo sistema.

3.4.3. PowerShell ir kompiuterizuotų saugumo politikų taisyklių atributai

Taisyklių atributų pavadinimai atitinka tikrinimo ir užtikrinimo PowerShell komandų parametrų pavadinimus. Apjungiant KSP tikrinimo / užtikrinimo funkcijų pavadinimą, taisyklės atributų pavadinimus bei jų reikšmes yra sugeneruojamos PowerShell komandos, kurių pagalba atitiktis yra tiek patikrinama, tiek užtikrinama. Svarbu paminėti, kad prototipo testavimo metu į KSP bus įtraukiami tik patys svarbiausi organizacijos saugai didelę įtaką turintys parametrai, tačiau esant poreikiui, galima pridėti ir visus, kuriuos leidžia tiek atitikties tikrinimo, tiek užtikrinimo funkcijos. Galimais laikomi yra tie parametrai, kuriuos kaip įvestį priima tiek tikrinimo, tiek užtikrinimo funkcijos.

3.4.4. *ADMXRule* tipo taisyklė

Administrative Template Rule (trump. *ADMXRule*) yra GP taisyklės tipas, kuris skirtas valdyti registrų raktų reikšmes. Manipuliavimas registrų raktų reikšmėmis gali paveikti tiek Active Directory vartotojus, tiek jų kompiuterius. Šių taisyklių pagalba galima konfigūruoti daugybę Windows OS saugumo nustatymų, įskaitant slaptažodžių reikalavimus, ugniasienės nustatymus, šifravim, tam tikrų funkcionalumų įjungimą / išjungimą. *ADMXRule* tipo taisyklės gali būti konfigūruojamos tiek per terminalinę, tiek per vartotojo sąsają „Group Policy Management“ programos pagalba. *ADMXRule* tipo taisyklė susideda iš žemiau išvardintų atributų:

- **Name** – GP pavadinimas;
- **Key** – registro pavadinimas;
- **ValueName** – registro reikšmės pavadinimas;
- **Type** – registro duomenų tipas;
- **Value** – registro reikšmė.

3.4 pav. pavaizduota *ADMXRule* struktūra XSD formatu.

```
<xs:schema attributeFormDefault="unqualified"
elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="ADMXRule">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="Name" type="xs:string" />
        <xs:element name="Key" type="xs:string" />
        <xs:element name="ValueName" type="xs:string" />
        <xs:element name="Type" type="xs:string" />
        <xs:element name="Value" type="xs:integer" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

3.4 pav. *ADMXRule* XML objekto struktūra

3.4.4.1. Atitikties tikrinimas

Get-GPRegistryValue yra PowerShell funkcija skirta patikrinti registrų reikšmes GP objekte. Sistema naudoja šią funkciją tikrinant *ADMXRule* taisyklės atitiktį. Kaip *ADMXRule* taisyklės panaudos atvejį galima pateikti būtinybę aktyvuoti ugniasienės naudojimą Domain profilyje. Apačioje pateiktas registro reikšmės tikrinimo PowerShell komandos pavyzdys:

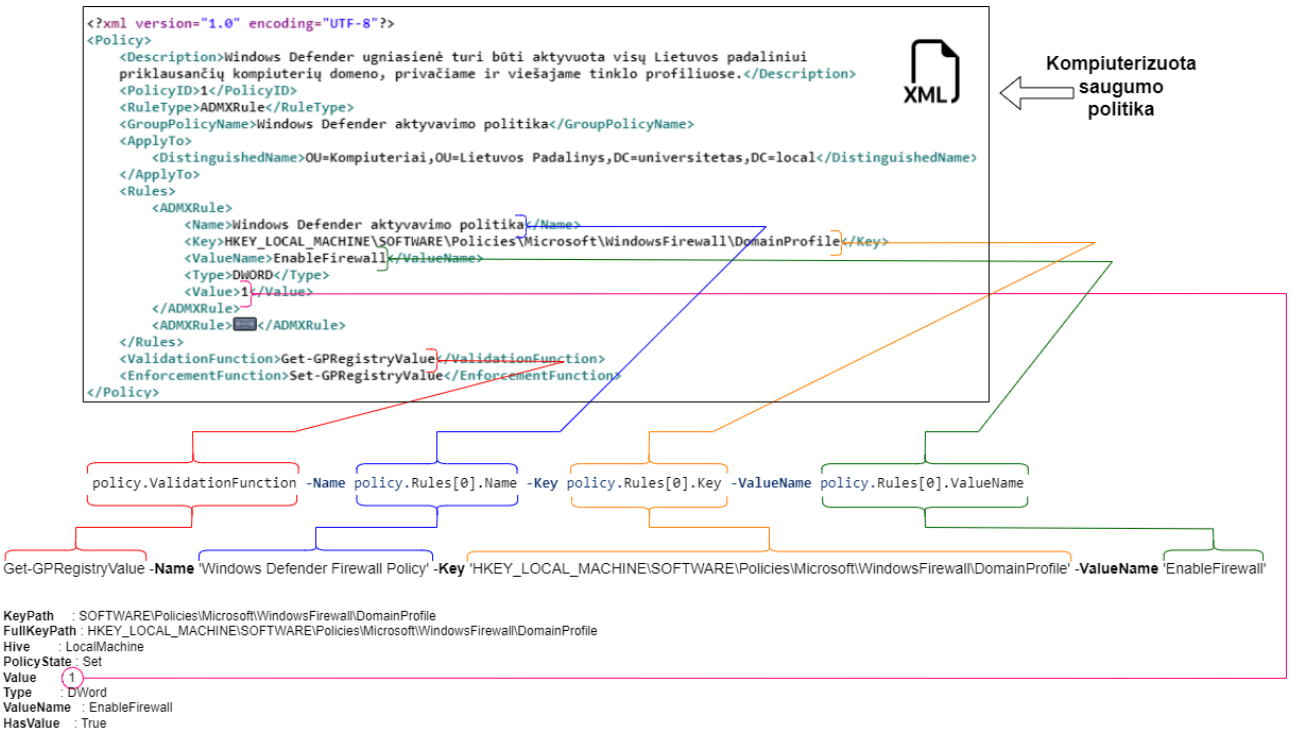
```
Get-GPRegistryValue
-Name 'Windows Defender Firewall aktyvavimo politika'
-Key 'HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\Domain-
Profile'
-ValueName 'EnableFirewall'
```

Pavaizduota komanda sugeneruoja išvestį, pagal kurią sistema nustato, ar registro reikšmė yra tokia, kokia yra nurodyta KSP taisyklėje. Išvesties pavyzdys pateiktas apačioje:

```
KeyPath     : SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile
FullKeyPath :
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile
Hive        : LocalMachine
PolicyState : Set
Value       : 1
Type        : DWord
ValueName   : EnableFirewall
HasValue    : True
```

Registras ir jo reikšmė yra identifikuojama pagal Key ir ValueName, o taisyklės atitiktis yra nustatoma pagal Value atributo reikšmę, kurią sistema ir tikrina.

3.4.4.2. Atitikties tikrinimo komandos generavimas



3.5 pav. *ADMXRule* taisyklės atitikties tikrinimo komandos generavimo schema

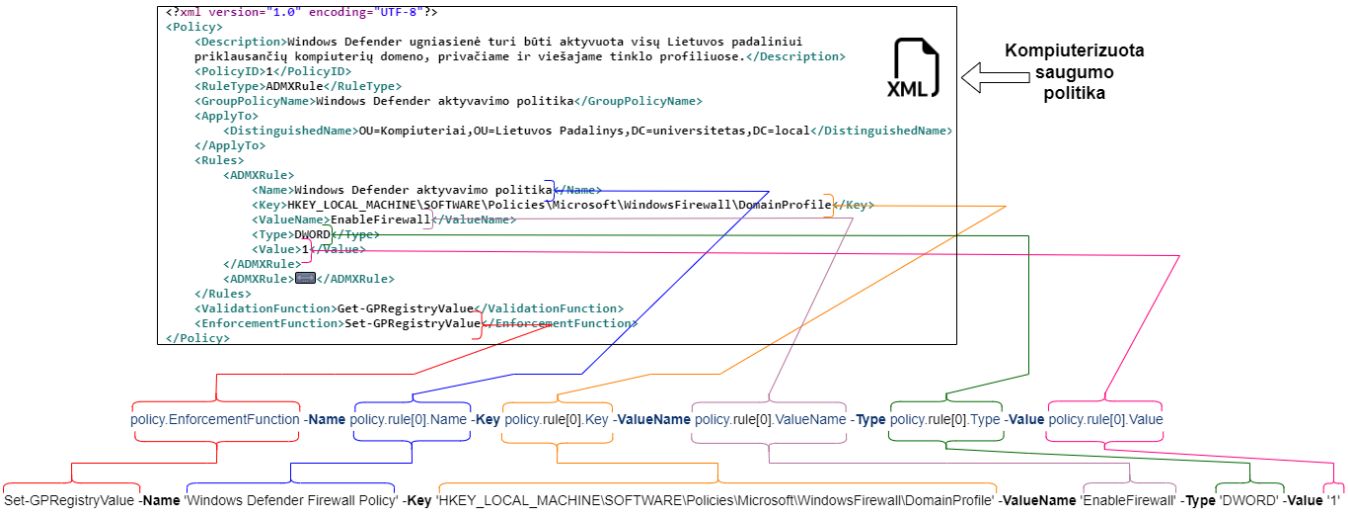
3.4.4.3. Atitikties užtikrinimas

Set-GPRegistryValue yra PowerShell funkcija skirta nustatyti registrų reikšmes. Sistema naudoja šią funkciją užtikrinant *ADMXRule* taisyklės atitiktį. Apačioje pateiktas registro reikšmės nustatymo PowerShell komandos pavyzdys:

```
Set-GPRegistryValue
-Name 'Windows Defender Firewall aktyvavimo politika'
-Key 'HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\Domain-
Profile'
-ValueName 'EnableFirewall'
-Type 'DWORD'
-Value 1
```

Paleidus komandą ir išvestyje negavus klaidų, sistema traktuoja, kad ADMXRule tipo taisyklės atitiktis buvo sėkmingai užtikrinta.

3.4.4.4. Atitikties užtikrinimo komandos generavimas



3.6 pav. *ADMXRule* taisyklės atitikties užtikrinimo komandos generavimo schema

3.4.5. *MWDProfileRule* tipo taisyklė

Microsoft Windows Defender Profile Rule (trump. *MWDProfileRule*) yra taisyklė, kuria nustatoma numatytoji Windows Defender ugniasienės elgsena su įeinančiu bei išeinančiu tinklo srautais. Jie pagal numatytuosius nustatymus gali būti leidžiami arba blokuojami ir gali būti konfigūruojami skirtingiems tinklo profiliams (Domain, Private arba Public). Visuotinai priimta ugniasienių praktika yra visą įeinantį ir taisyklių neatitinkantį srautą blokuoti, o išeinantį – leisti. Tai yra labai svarbu sukonfigūruoti prieš pradedant kurti ugniasienės taisykles. *MWDProfileRule* tipo taisyklė susideda iš žemiau išvardintų atributų:

- **Name** – tinklo profilio pavadinimas;
- **PolicyStore** – GP saugyklos pavadinimas, susidedantis iš domeno ir GP pavadinimų;
- **DefaultInboundAction** – atributas, nusakantis elgseną su įeinančiu tinklo srautu;
- **AllowLocalFirewallRules** – atributas, nusakantis elgseną su domenui priklausančio kompiuterio lokaliomis ugniasienės taisyklėmis (leisti ar drausti);

- **AllowUserApps** – atributas, nusakantis leidimą arba draudimą įrašyti bei naudoti GP neįvardytą programinę įrangą ir atverti jos veikimui reikalingus prievadus domenui priklausančiame kompiuteryje;
- **AllowUserPorts** – atributas, nusakantis leidimą arba draudimą atverti prievadus domenui priklausančiame kompiuteryje;
- **Enabled** – atributas, nurodantis taisyklės įgalinimo statusą.

3.7 pav. pavaizduota *MWDProfileRule* struktūra XSD formatu.

```
<xs:schema attributeFormDefault="unqualified"
elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="MWDProfileRule">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="Name" type="xs:string" />
        <xs:element name="PolicyStore" type="xs:string" />
        <xs:element name="DefaultInboundAction" type="xs:string" />
        <xs:element name="AllowLocalFirewallRules" type="xs:boolean" />
        <xs:element name="AllowUserApps" type="xs:boolean" />
        <xs:element name="AllowUserPorts" type="xs:boolean" />
        <xs:element name="Enabled" type="xs:boolean" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

3.7 pav. *MWDProfileRule* XML objekto struktūra

3.4.5.1. Atitikties tikrinimas

Get-NetFirewallProfile yra PowerShell funkcija skirta patikrinti tinklo profilių (Domain, Private, Public) konfigūraciją. Sistema naudoja šią funkciją tikrinant *MWDProfileRule* taisyklės atitiktį. Apačioje pateiktas atitikties tikrinimo PowerShell komandos pavyzdys:

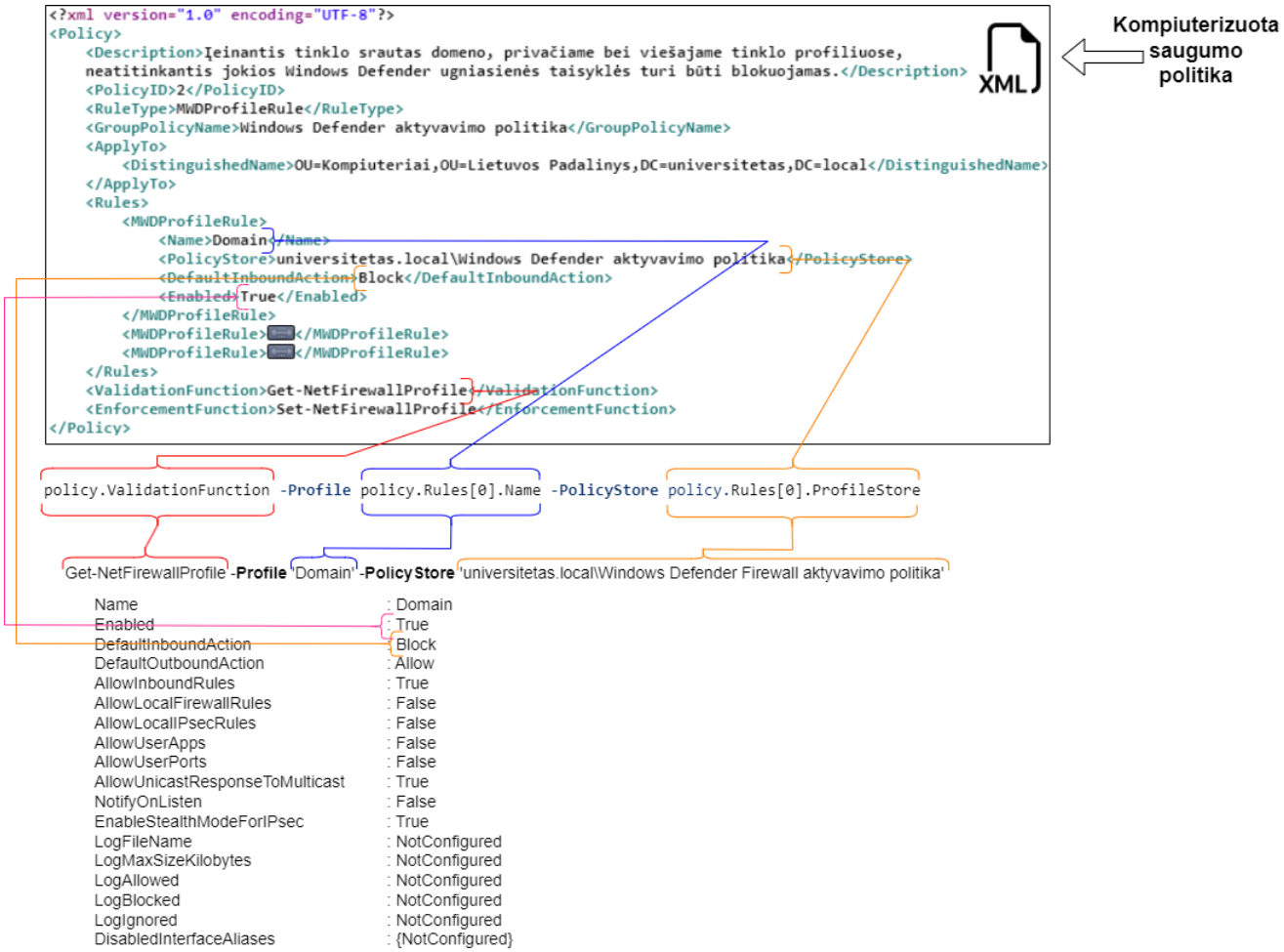
```
Get-NetFirewallProfile
-Profile 'Domain'
-PolicyStore 'universitetas.local\Windows Defender Firewall aktyvavimo poli-
tika'
```

Pavaizduota komanda sugeneruoja išvestį, pagal kurią sistema nustato, ar tinklo profilio konfigūracija atitinka KSP taisykles. Išvesties pavyzdys pateiktas apačioje:

```
Name                                  : Domain
Enabled                               : True
DefaultInboundAction                  : Block
DefaultOutboundAction                 : Allow
AllowInboundRules                     : True
AllowLocalFirewallRules               : False
AllowLocalIPsecRules                  : False
AllowUserApps                         : False
AllowUserPorts                        : False
AllowUnicastResponseToMulticast       : True
NotifyOnListen                        : False
EnableStealthModeForIPsec             : True
LogFileName                           : NotConfigured
LogMaxSizeKilobytes                   : NotConfigured
LogAllowed                            : NotConfigured
LogBlocked                            : NotConfigured
LogIgnored                            : NotConfigured
DisabledInterfaceAliases              : {NotConfigured}
```

Sistema sugeneravus išvestį tikrina kiekvienos *MWDProfileRule* taisyklėje aprašyto ir išvestyje esančio atributo reikšmę.

3.4.5.2. Atitikties tikrinimo komandos generavimas



3.8 pav. *MWDProfileRule* taisyklės atitikties tikrinimo komandos generavimo schema

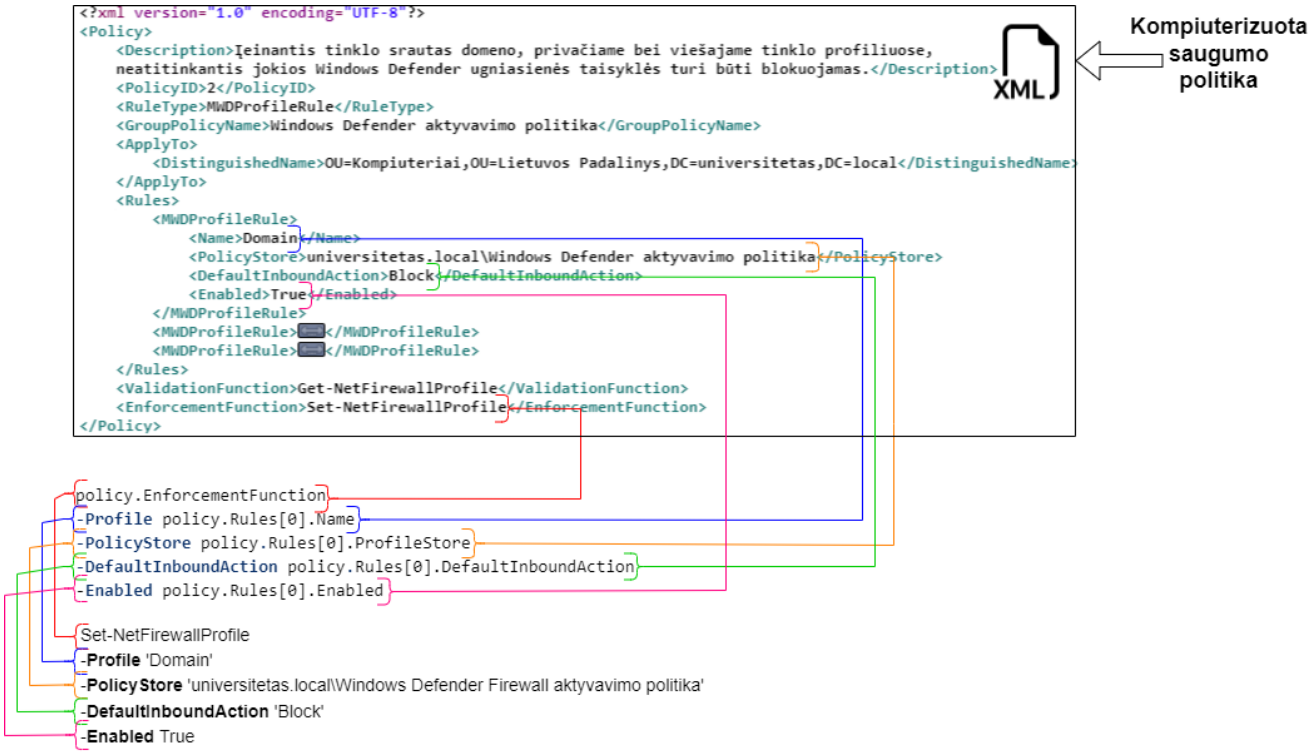
3.4.5.3. Atitikties užtikrinimas

Set-NetFirewallProfile yra PowerShell funkcija skirta tinklo profilių nustatymų keitimui. Sistema naudoja šią funkciją užtikrinant *MWDProfileRule* taisyklės atitiktį. Apačioje pateiktas atitikties užtikrinimo PowerShell komandos pavyzdys:

```
Set-NetFirewallProfile
-Profile 'Domain'
-PolicyStore 'universitetas.local\Windows Defender Firewall aktyvavimo poli-
tika'
-DefaultInboundAction 'Block'
-AllowLocalFirewallRules False
-AllowUserApps False
-AllowUserPorts False
-Enabled True
```

Paleidus komandą ir išvestyje negavus klaidų, sistema traktuoja, kad *MWDProfileRule* tipo taisyklės atitiktis buvo sėkmingai užtikrinta.

3.4.5.4. Atitikties užtikrinimo komandos generavimas



3.9 pav. *MWDProfileRule* taisyklės atitikties užtikrinimo komandos generavimo schema

3.4.6. *MWDTrafficRule* tipo taisyklė

Microsoft Windows Defender Traffic Rule (trump. *MWDTrafficRule*) yra taisyklė, kuri nustato kaip Windows Defender ugniasienė tvarko tam tikrus kriterijus atitinkantį įeinantį ir išeinantį tinklo srautus. Kadangi pagal numatytuosius *MWDProfileRule* nustatymus visas įeinantis tinklo srautas neatitinkantis jokios aprašytos taisyklės kriterijų yra blokuojamas, o išeinantis leidžiamas, šių *MWDTrafficRule* tipo taisyklių tikslas – aprašyti išimtis (taisykles) įeinančiam bei išeinančiam tinklo srautui. Pvz. yra vienintelė įeinančio srauto taisyklė, leidžianti įeinantį srautą tik iš 80 bei 443 prievadų, tai reiškia, kad visais kitais prievadais komunikacija yra neįmanoma, nes taisyklių

neatitinkantys įeinantys tinklo srautai yra blokuojami. *MWDProfileRule* tipo taisyklė susideda iš žemiau išvardintų atributų:

- **PolicyStore** – GP saugyklos pavadinimas, susidedantis iš domeno ir GP pavadinimų;
- **Name** – unikalus taisyklės identifikatorius;
- **Profile** – tinklo profilio pavadinimas;
- **DisplayName** – taisyklės pavadinimas;
- **Direction** – tinklo srauto kryptis (įeinantis arba išeinantis), kuriai taisyklė yra taikoma;
- **Action** – atributas, kuriuo nusakoma leisti ar blokuoti taisyklę atitinkantį tinklo srautą;
- **LocalAddress** – vietinio įrenginio IP adresas (-ai) arba IP adresų sritis, kuriai taikoma taisyklė;
- **RemoteAddress** – nutolusio įrenginio IP adresas (-ai) arba IP adresų sritis, kuriai taikoma taisyklė;
- **LocalPort** – vietinio įrenginio prievadas (-ai) arba prievadų sritis, kuriai taikoma taisyklė;
- **RemotePort** – nutolusio įrenginio prievadas (-ai) arba prievadų sritis, kuriai taikoma
- **Program** – programa, kuriai taikoma taisyklė;
- **Protocol** – tinklo protokolas;
- taisyklė;
- **Enabled** – atributas, nurodantis taisyklės įgalinimo statusą.

3.10 pav. pavaizduota *MWDTrafficRule* struktūra XSD formatu.

```
<xs:schema attributeFormDefault="unqualified"
elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="MWDTrafficRule">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="PolicyStore" type="xs:string" />
        <xs:element name="Name" type="xs:string" />
        <xs:element name="Profile" type="xs:string" />
        <xs:element name="DisplayName" type="xs:string" />
        <xs:element name="Direction" type="xs:string" />
        <xs:element name="Action" type="xs:string" />
        <xs:element name="LocalAddress" type="xs:string" />
        <xs:element name="RemoteAddress" type="xs:string" />
        <xs:element name="LocalPort" type="xs:string" />
        <xs:element name="RemotePort" type="xs:string" />
        <xs:element name="Protocol" type="xs:string" />
        <xs:element name="Program" type="xs:string" />
        <xs:element name="Enabled" type="xs:boolean" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

3.10 pav. *MWDTrafficRule* XML objekto struktūra

3.4.6.1. Atitikties tikrinimas

Get-NetFirewallRule yra PowerShell funkcija skirta surasti ir grąžinti paieškos kriterijos atitinkančias ugniasienės taisykles. Tačiau *MWDTrafficRule* taisyklės atitikties patikrinimui nepakanka tik šios funkcijos, taip pat reikalingos ir kitos *NetSecurity* moduliui priklausančios funkcijos:

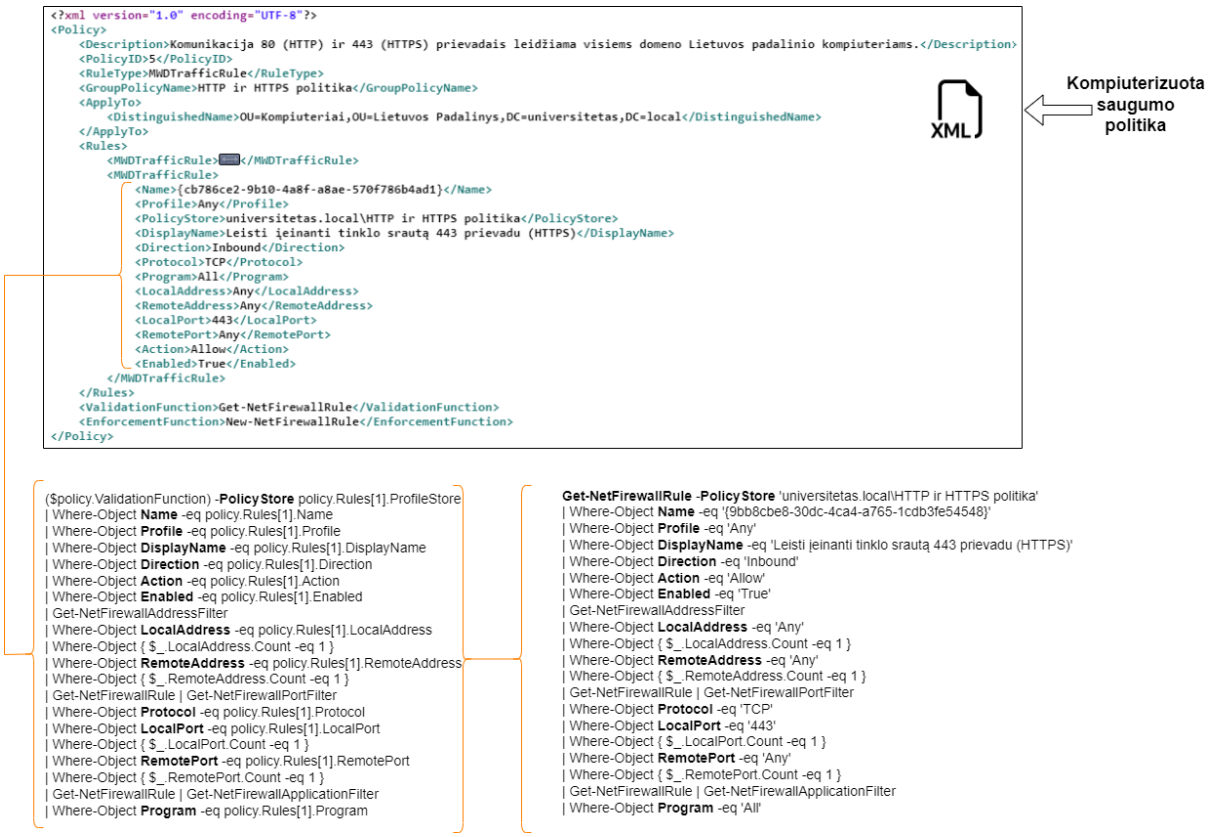
- Get-NetFirewallAddressFilter,
- Get-NetFirewallPortFilter,
- Get-NetFirewallApplicationFilter,

grąžinančios kitus specifinius taisyklės realizacijos atributus. Sistema į atitikties patikros komandą įtraukia tik tuos atributus, kurie aprašyti taisyklėje. Apačioje pateiktas atitikties tikrinimo PowerShell komandos pavyzdys:

```
Get-NetFirewallRule -PolicyStore 'universitetas.local\HTTP ir HTTPS politika'
| Where-Object Name -eq '{9bb8cbe8-30dc-4ca4-a765-1cdb3fe54548}'
| Where-Object Profile -eq 'Any'
| Where-Object DisplayName -eq 'Leisti įeinanti tinklo srautą 443 prievadu
(HTTPS)'
| Where-Object Direction -eq 'Inbound'
| Where-Object Action -eq 'Allow'
| Where-Object Enabled -eq 'True'
| Get-NetFirewallAddressFilter
| Where-Object LocalAddress -eq 'Any'
| Where-Object { $_.LocalAddress.Count -eq 1 }
| Where-Object RemoteAddress -eq 'Any'
| Where-Object { $_.RemoteAddress.Count -eq 1 }
| Get-NetFirewallRule | Get-NetFirewallPortFilter
| Where-Object Protocol -eq 'TCP'
| Where-Object LocalPort -eq '443'
| Where-Object { $_.LocalPort.Count -eq 1 }
| Where-Object RemotePort -eq 'Any'
| Where-Object { $_.RemotePort.Count -eq 1 }
| Get-NetFirewallRule | Get-NetFirewallApplicationFilter
| Where-Object Program -eq 'All'
```

Paleidus komandą ir išvestyje gavus paieškos kriterijus atitinkančios taisyklės objektą, sistema traktuoja, kad tokia *MWDTrafficRule* taisyklė egzistuoja egzistuoja.

3.4.6.2. Atitikties tikrinimo komandos generavimas




```
<?xml version="1.0" encoding="UTF-8"?>
<Policy>
    <Description>Komunikacija 80 (HTTP) ir 443 (HTTPS) prievadais leidžiama visiems domeno Lietuvos padalinio kompiuteriams.</Description>
    <PolicyID>5</PolicyID>
    <RuleType>MWDTrafficRule</RuleType>
    <GroupPolicyName>HTTP ir HTTPS politika</GroupPolicyName>
    <ApplyTo>
        <DistinguishedName>OU=Kompiuteriai,OU=Lietuvos Padalinys,DC=universitetas,DC=local</DistinguishedName>
    </ApplyTo>
    <Rules>
        <MWDTrafficRule>[redacted]</MWDTrafficRule>
        <MWDTrafficRule>
            <Name>{cb786ce2-9b10-4a8f-a8ae-570f786b4ad1}</Name>
            <Profile>Any</Profile>
            <PolicyStore>universitetas.local\HTTP ir HTTPS politika</PolicyStore>
            <DisplayName>Leisti įeinanti tinklo srautą 443 prievadu (HTTPS)</DisplayName>
            <Direction>Inbound</Direction>
            <Protocol>TCP</Protocol>
            <Program>All</Program>
            <LocalAddress>Any</LocalAddress>
            <RemoteAddress>Any</RemoteAddress>
            <LocalPort>443</LocalPort>
            <RemotePort>Any</RemotePort>
            <Action>Allow</Action>
            <Enabled>True</Enabled>
        </MWDTrafficRule>
    </Rules>
    <ValidationFunction>Get-NetFirewallRule</ValidationFunction>
    <EnforcementFunction>New-NetFirewallRule</EnforcementFunction>
</Policy>
```

3.11 pav. *MWDTrafficRule* taisyklės atitikties tikrinimo komandos generavimo schema

3.4.6.3. Atitikties užtikrinimas

New-NetFirewallRule yra PowerShell komanda naudojama naujos ugniasienės arba *MWDTrafficRule* taisyklės sukūrimui. Svarbu paminėti, jog aptikus neatitiktį taisyklė nėra modifikuojama, o ištrinama ir sukuriama iš naujo. Apačioje pateiktas atitikties užtikrinimo (taisyklės sukūrimo) PowerShell komandos pavyzdys:

```
New-NetFirewallRule
-Profile 'Any'
-PolicyStore 'universitetas.local\HTTP ir HTTPS politika'
-DisplayName 'Leisti įeinanti tinklo srautą 443  prievadu (HTTPS)'
-Direction 'Inbound'
-Protocol 'TCP'
-Program 'All'
-LocalAddress 'Any'
-RemoteAddress 'Any'
-LocalPort '443'
-RemotePort 'Any'
-Action 'Allow'
-Enabled 'True'
```

Paleidus komandą ir išvestyje negavus klaidos, sistema laiko, kad *MWDTrafficRule* taisyklės atitiktis buvo sėkmingai užtikrinta.

3.4.6.4. Atitikties užtikrinimo komandos generavimas

3.12 pav. *MWDTrafficRule* taisyklės atitikties užtikrinimo komandos generavimo schema

3.4.7. Neatitikties tipai

Kiekvieno tipo taisyklei yra priskiriamas neatitikties tipas, kurie bus atvaizduojami sistemos sugeneruotoje atitikties ataskaitoje. Neatitikties objektai ir jų paaiškinimai pateikti apačioje:

- **Missing_GPO** – GP neegzistavimo neatitiktis;
- **Disabled_GPO** – GP neįgalinimo neatitiktis;
- **GPO_appliance_to_OU_Incompliance** – GP taikymo OV neatitiktis;
- **ADMXRule_Incompliance** – *ADMXRule* tipo taisyklės neatitiktis;
- **MWDProfileRule_Incompliance** – *MWDProfileRule* tipo taisyklės neatitiktis;
- **MWDTrafficRule_Incompliance** – *MWDTrafficRule* tipo taisyklės neatitiktis;
- **Redundant_MWDTrafficRule** – perteklinės ar nereikalingos *MWDTrafficRule* tipo taisyklės egzistavimo neatitiktis.

3.1 lentelėje pavaizduota praeitame skyrelyje pristatytų neatitikties objektų struktūra. Pagal poreikį į neatitikties objekto sudėtį gali būti įtraukiami papildomi atributai siekiant geriau informuoti sistemos naudotoją apie tam tikrą neatitiktį. Pliusas lentelėje reiškia, kad atributas įeina į neatitikties objekto sudėtį, o minusas – neįeina.

3.1 lentelė. Neatitikties objektų atributų lentelė

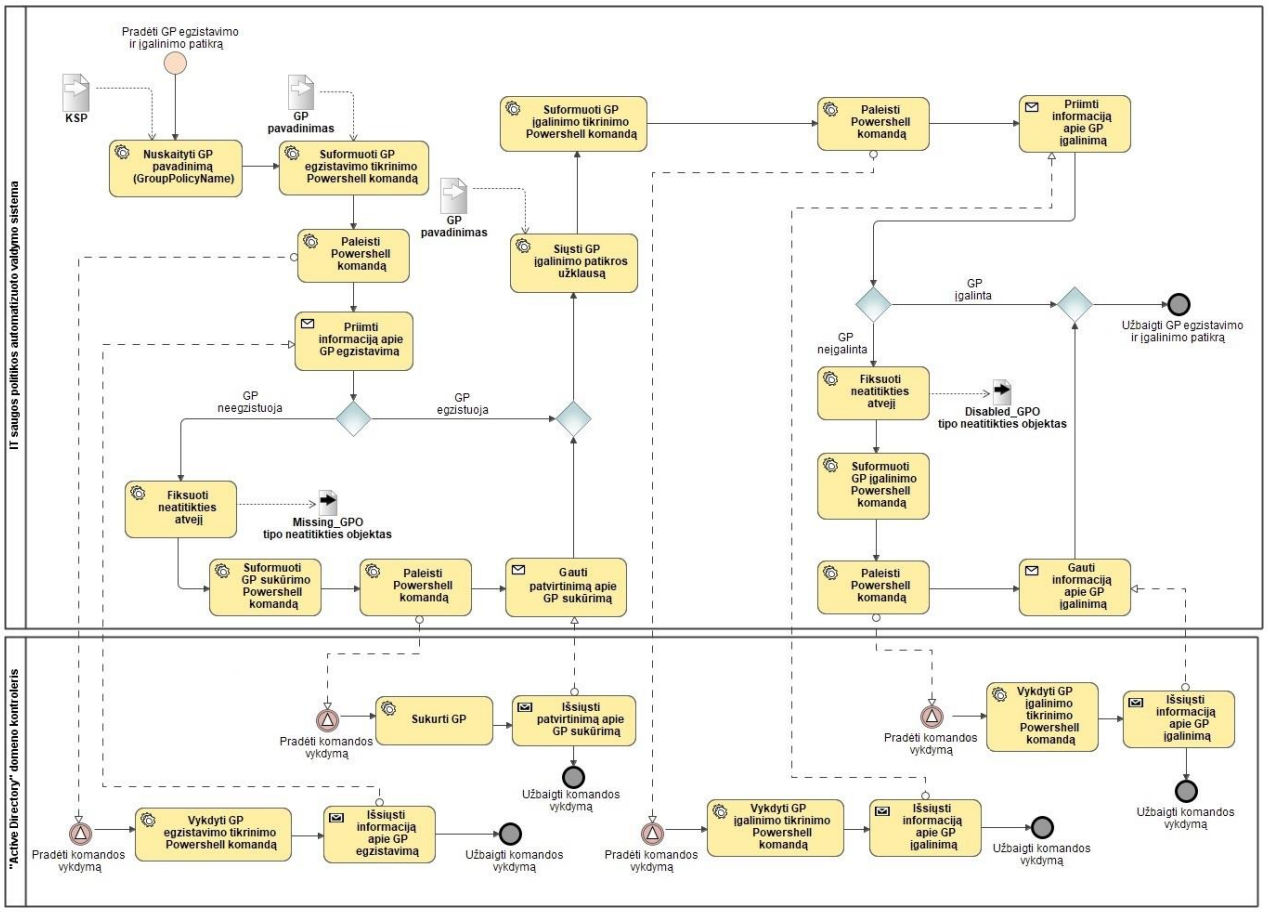
	Missing _OU	**Disabled _OU**	**GPO _appliance _to_OU _Incompliance**	**ADMX Rule _Incompliance**	**MWDProfile Rule _Incompliance**	**MWDTraffic Rule _Incompliance**	**Redundant _MWDTraffic Rule _Incompliance**
Neatitikties ID	+	+	+	+	+	+	+
Neatitikties Tipas	+	+	+	+	+	+	+
Domenas	+	+	+	+	+	+	+
GP	+	+	+	+	+	+	+
KSP ID	+	+	+	+	+	+	-
Taisyklės eilės numeris	-	-	-	+	+	+	-
Tekstinės saugumo politikos aprašymas	-	-	-	+	+	+	-
OV	-	-	-	-	-	-	-
Neatitikties aprašymas	+	+	+	+	+	+	+
Aptikimo laikas	+	+	+	+	+	+	+
Atitiktis užtikrinta	+	+	+	+	+	+	+

3.5. Grupės politikos egzistavimo ir įgalinimo atitikties tikrinimas ir užtikrinimas

Proceso įvestis yra KSP. Taisyklių atitikties tikrinimas vyksta žemiau išvardinta eilės tvarka:

1. Iš KSP yra nuskaitomas GP pavadinimas (*GroupPolicyName* atributo reikšmė);
2. Tikrinama, ar GP tokiu pavadinimu egzistuoja;
3. Jei GP neegzistuoja, sukuriamas *Missing_GPO* tipo neatitikties objektas;
4. Jei GP neegzistuoja, GP yra sukūriama;
5. Tikrinama, ar GP tokiu pavadinimu yra įgalinta;
6. Jei GP neįgalinta, sukuriamas *Disabled_GPO* tipo neatitikties objektas;
7. Jei GP neįgalinta, GP yra įgalinama.

Veiklos procesas pavaizduotas 3.13 pav.



3.13 pav. Tikrinti ir užtikrinti grupės politikos egzistavimą ir įgalinimą

Proceso metu naudojamos funkcijos pateiktos priede Nr. 1 ir Nr. 2. Proceso rezultatas – užregistruotos ir pašalintos *Missing_GPO* ir *Disabled_GPO* neatitiktys.

3.6. Grupės politikos taikymo organizaciniams vienetams atitikties tikrinimas ir užtikrinimas

3.6.1. Organizacinis vienetas ir kompiuterizuota saugumo politika

KSP aprašo GP taisykles, o GP yra taikomos OV. OV gali būti interpretuojami kaip tam tikro tipo vartotojų ar įrenginių grupės, padaliniai, domenai ir pan. Kai GP yra pritaikoma OV, joje atlikta konfigūracija yra pritaikoma visiems OV konteineryje esantiems objektams. OV KSP saugomi *ApplyTo* sąraše, kurį sudaro *DistinguishedName* reikšmės. 3.14 pav. pavaizduota kompiuterizuotos saugumo politikos ištrauka su *DistinguishedName* tipo reikšmėmis.

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy>
  <Description>Politikos_aprašymas</Description>
  <PolicyID>Politikos_ID</PolicyID>
  <RuleType>Taisyklių_tipas</RuleType>
  <GroupPolicyName>GPO_pavadinimas</GroupPolicyName>
  <ApplyTo>
    <DistinguishedName>OU=Buhalterijos skyrius,OU=Kompiuteriai,OU=Lietuvos Padalinys,DC=universitetas,DC=local</DistinguishedName>
    <DistinguishedName>OU=Pardavimų skyrius,OU=Kompiuteriai,OU=Lietuvos Padalinys,DC=universitetas,DC=local</DistinguishedName>
  </ApplyTo>
```

3.14 pav. Organizaciniai vienetai kompiuterizuotoje saugumo politikoje

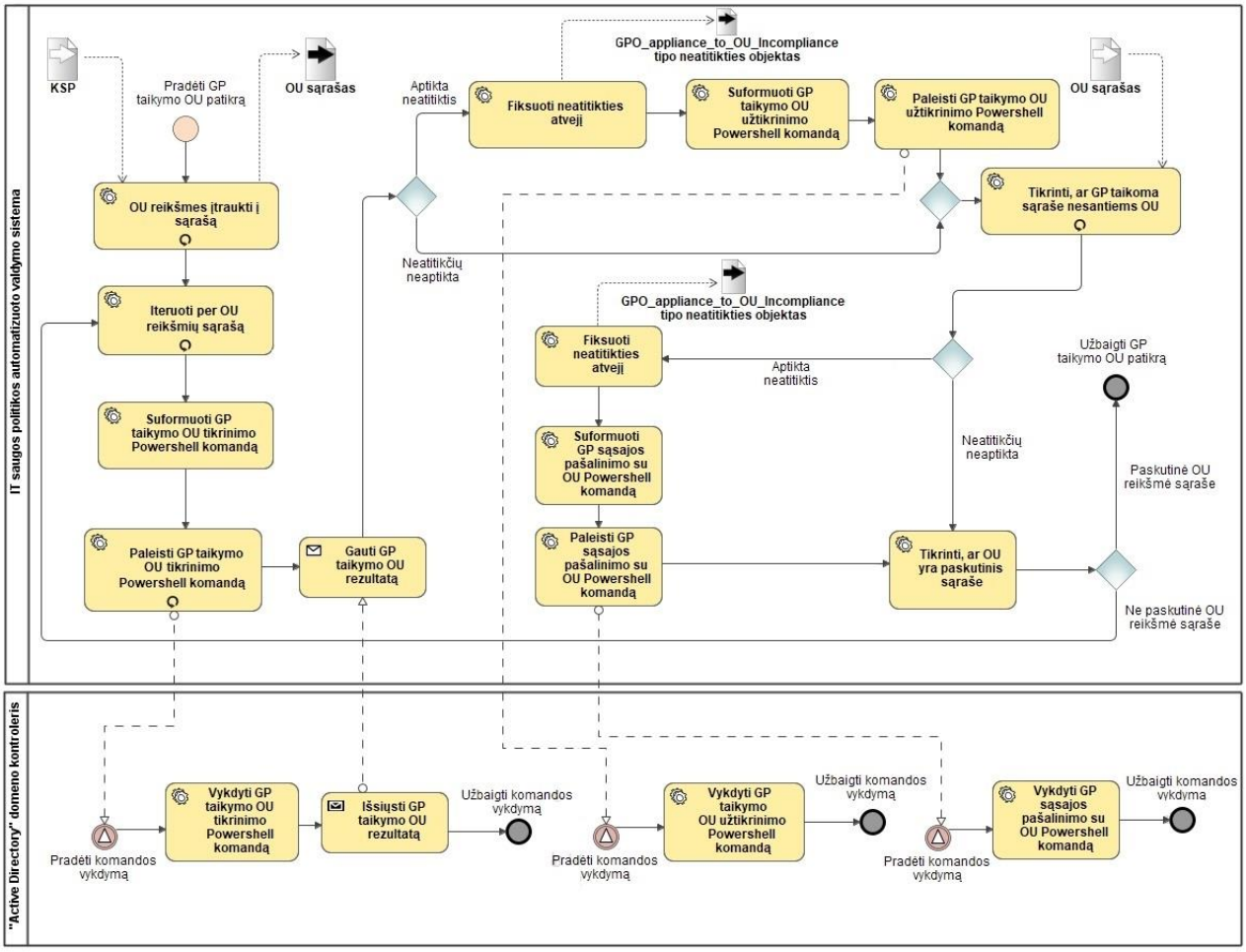
Pirmąjį sąrašo elementą galima interpretuoti kaip universitetas.local domeno Lietuvos padalinio Buhalterijos skyriaus kompiuterių OV. Antrasis masyvo elementas nuo pirmojo skiriasi tik tuo, kad skyrius yra ne pardavimų, o buhalterijos. Taigi, *ApplyTo* sąrašo reikšmės nurodo, kuriem OV GP turi būti taikoma. Kaskart pradėjus KSP apdorojimą sistema tikrina GP priskyrimus OV.

3.6.2. Veiklos procesas

Proceso įvestis yra KSP. GP taikymo OV atitikties tikrinimo ir užtikrinimo procesas vyksta iteraciniu principu. GP taikymo OV atitikties tikrinimas vyksta žemiau išvardinta eilės tvarka:

1. Iš KSP yra nuskaitomas OV sąrašas (*ApplyTo* sąraše esančios *DistinguishedName* reikšmės);
2. Tikrinama, ar einamoji GP pritaikyta teisingiems, KSP nurodytiems OU;
3. Jei GP nėra taikoma einamajam OU, sukuriamas *GPO_appliance_to_OU_Incompliance* tipo neatitikties objektas;
4. GP priskiriama OU;
5. Tikrinama, ar einamoji GP nėra papildomai taikoma kitiems KSP nenurodytiems OU;
6. Jei GP yra taikoma papildomam KSP nenurodytam OU, sukuriamas *GPO_appliance_to_OU_Incompliance* tipo neatitikties objektas;
7. Pašalinama GPO su OU sąsaja.

Veiklos procesas pavaizduotas 3.15 pav.



3.15 pav. Tikrinti ir užtikrinti grupės politikos taikymo organizaciniam vienetui atitiktį

Proceso metu naudojamos funkcijos pateiktos priede Nr. 3 ir Nr. 4. Proceso rezultatas – užregistruotos ir pašalintos *GPO_appliance_to_OU_Incompliance* neatitiktys.

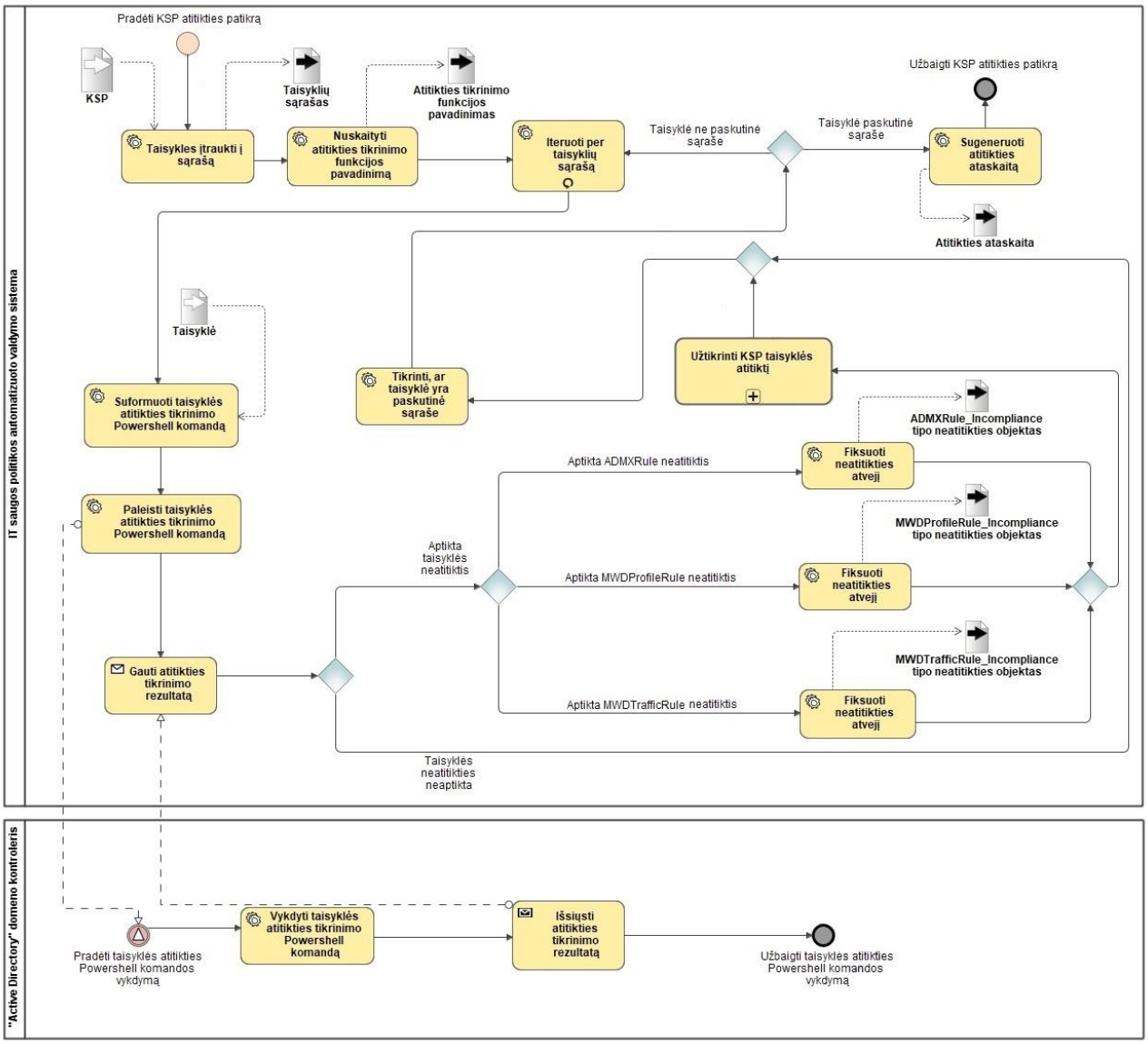
3.7. Taisyklių atitikties tikrinimas ir užtikrinimas

3.7.1. Taisyklių atitikties tikrinimo procesas

Proceso įvestis yra KSP. Taisyklių atitikties tikrinimas vyksta žemiau išvardinta eilės tvarka:

1. Iš KSP yra nuskaitomas taisyklių sąrašas;
2. Iš KSP yra nuskaitomas atitikties tikrinimo funkcijos pavadinimas;
3. Tikrinama einamosios taisyklės atitiktis;
4. Jei aptinkama einamosios taisyklės neatitiktis, priklausomai nuo jos tipo yra sukuriamas neatitikties objektas;
5. Einamajai taisyklei yra iškviečiamas KSP taisyklės užtikrinimo procesas;
6. Sugeneruojama atitikties ataskaita.

Veiklos procesas pavaizduotas 3.16 pav.



3.16 pav. Tikrinti kompiuterizuotos saugumo politikos taisyklių atitiktį

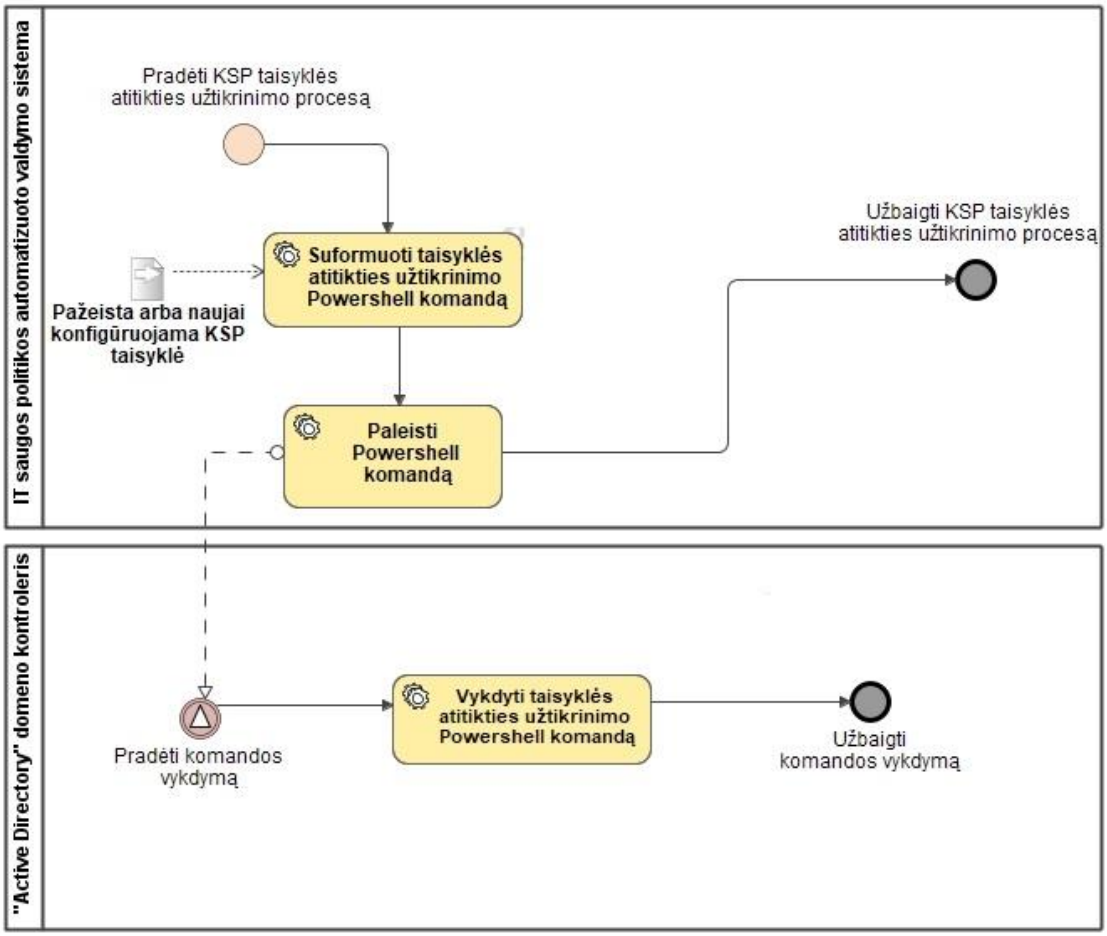
Proceso metu naudojamos funkcijos pateiktos priede Nr. 5, Nr. 6 ir Nr. 7. Proceso rezultatas – užregistruotos ir pašalintos *ADMXRule_Incompliance, MWDProfileRule_Incompliance, MWDTrafficRule_Incompliance* tipų neatitiktys.

3.7.2. Taisyklės atitikties užtikrinimo procesas

Proceso įvestis yra pažeista arba naujai konfigūruojama KSP taisyklė. Procesas vyksta žemiau išvardinta eilės tvarka:

1. Procesui perduodamas pažeistos arba naujai konfigūruojamos taisyklės objektas;
2. Suformuojama taisyklės atitikties užtikrinimo PowerShell komanda;
3. PowerShell komanda paleidžiama.

Įvykdžius šiuos žingsnius ir komandos vykdyme neaptikus klaidų sistema laiko, kad taisyklės atitiktis užtikrinta sėkmingai. Kitą kartą tikrinant pažeisto / naujai sukonfigūruotos KSP taisyklės atitiktį ji nebeturėtų būti aptinkama, nebent iki kito tikrinimo bus padaroma žmogiškoji klaida ir taisyklės konfigūracija sugadinama žmogaus. Veiklos procesas pavaizduotas 3.17 pav.



3.17 pav. Užtikrinti kompiuterizuotos saugumo politikos taisyklės atitiktį

Proceso metu sistemos generuojamose komandose naudojamos PowerShell funkcijos:

- Set-GPRegistryValue;
- Set-NetFirewallProfile;
- New-NetFirewallRule.

Proceso rezultatas – užtikrinta *ADMXRule*, *MWDProfileRule*, *MWDTrafficRule* taisyklių atitiktis.

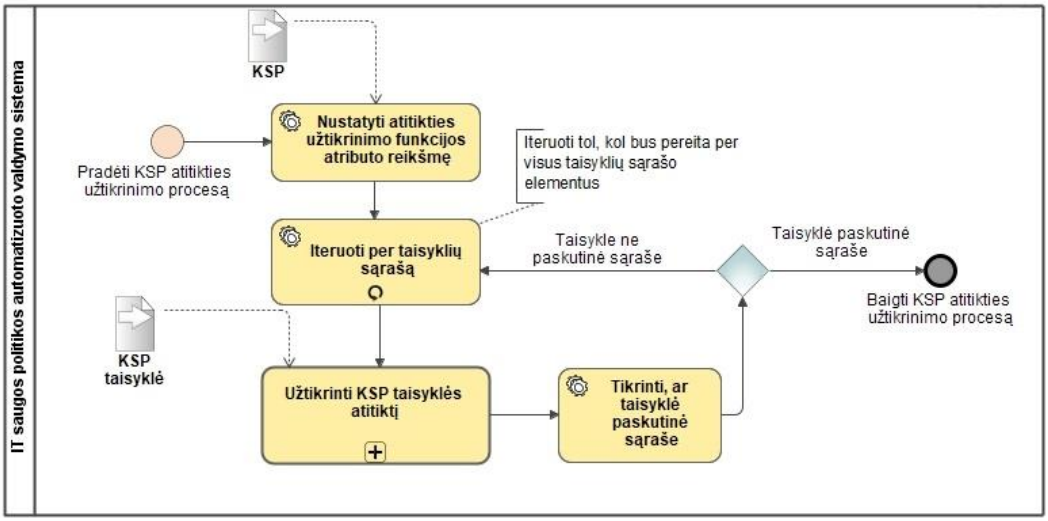
3.8. Kompiuterizuotos saugumo politikos atitikties užtikrinimas

3.8.1. Atitikties užtikrinimo procesas

Proceso įvestis yra KSP. KSP atitikties užtikrinimas vyksta žemiau išvardinta eilės tvarka:

1. Nustatomas atitikties užtikrinimo funkcijos pavadinimas;
2. Pradedamas iteravimas per taisyklių sąrašą;
3. Kiekvienai taisyklei iškviečiamas KSP taisyklės užtikrinimo procesas.

Veiklos procesas pavaizduotas 3.18 pav.

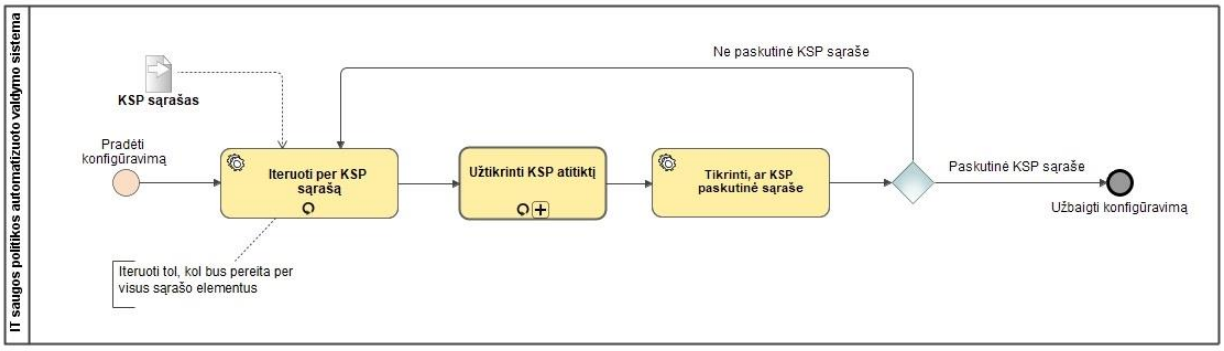


3.18 pav. Užtikrinti kompiuterizuotos saugumo politikos atitiktį

Proceso rezultatas – užtikrinta KSP (visų jos taisyklių) atitiktis.

3.8.2. Politikų sukonfigūravimas

Atliekant visų KSP konfigūraciją nuo pradžių yra užtikrinama kiekvienos iš jų atitiktis. Atitikties tikrinimas yra praleidžiamas, kadangi atliekama pradinė Active Directory domeno kontrolerio konfigūracija. Veiklos procesas pavaizduotas 3.19 pav.



3.19 pav. Konfigūruoti pagal kompiuterizuotas saugumo politikas

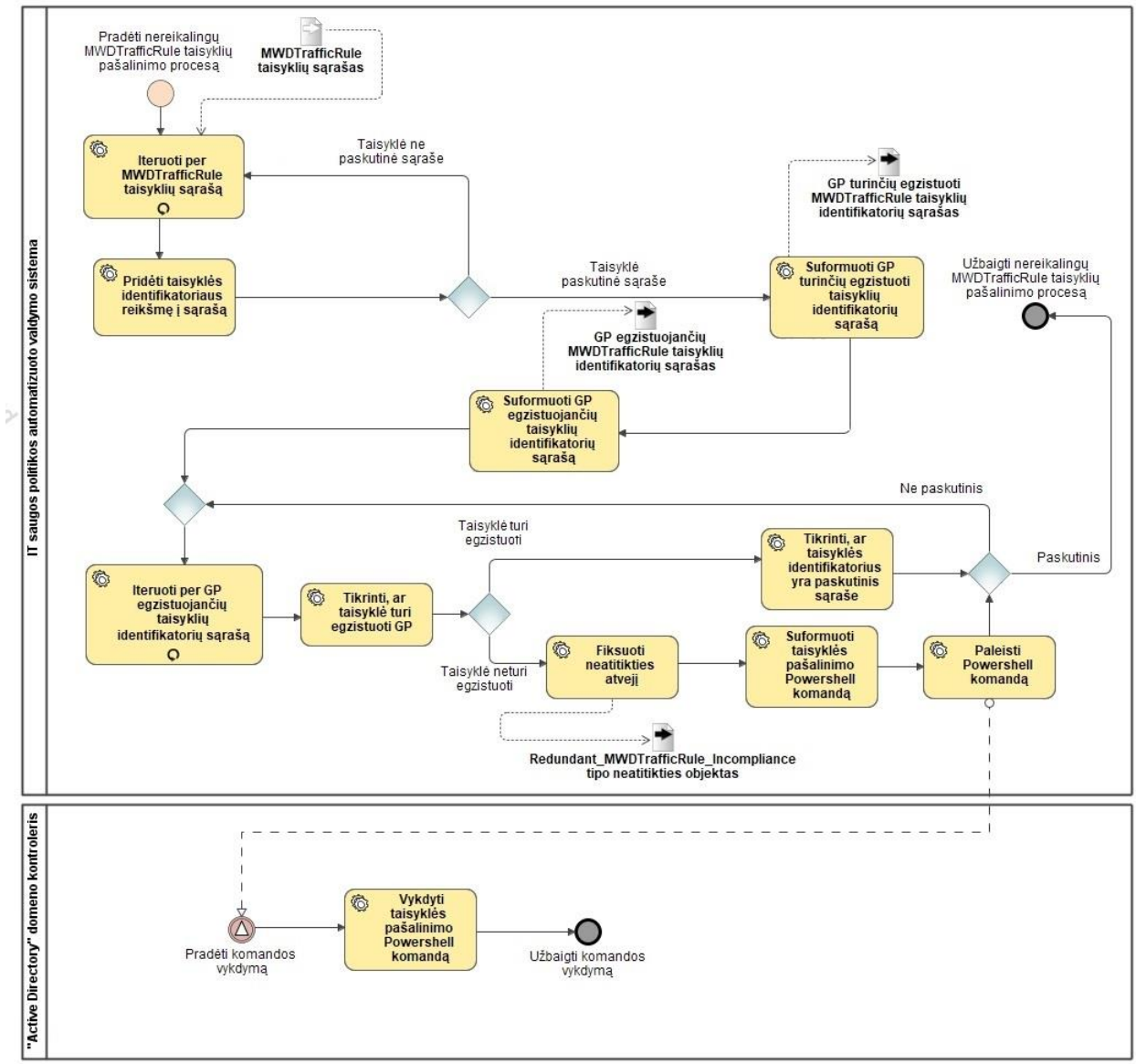
Proceso rezultatas – užtikrinta visų KSP atitiktis.

3.9. Nereikalingų *MWDTrafficRule* neegzistavimo užtikrinimas

Sistema geba nustatyti ir pašalinti nereikalingas KSP *MWDTrafficRule* taisykles, kurios gali kelti grėsmę organizacijos tinklo saugai. Proceso įvestis yra *MWDTrafficRule* tipo taisyklių sąrašas. Procesas vyksta žemiau išvardinta eilės tvarka:

1. Nuskaičius KSP sukurti PowerShell duomenų struktūrą, susidedančią iš GP ir toje GP turinčių egzistuoti *MWDTrafficRule* tipo taisyklių identifikatorių sąrašo (PowerShell *Tuple* duomenų struktūra);
2. Sukurti pirmam žingsniui analogišką PowerShell duomenų struktūrą, susidedančią iš GP ir toje GP šiuo metu egzistuojančių *MWDTrafficRule* unikalių taisyklių identifikatorių sąrašo (PowerShell *Tuple* duomenų struktūra);
3. Ieškoti taisyklių, kurios egzistuoja nors pagal KSP neturėtų egzistuoti ir tokias taisykles pašalinti iš GP.

Veiklos procesas pavaizduotas 3.20 pav.

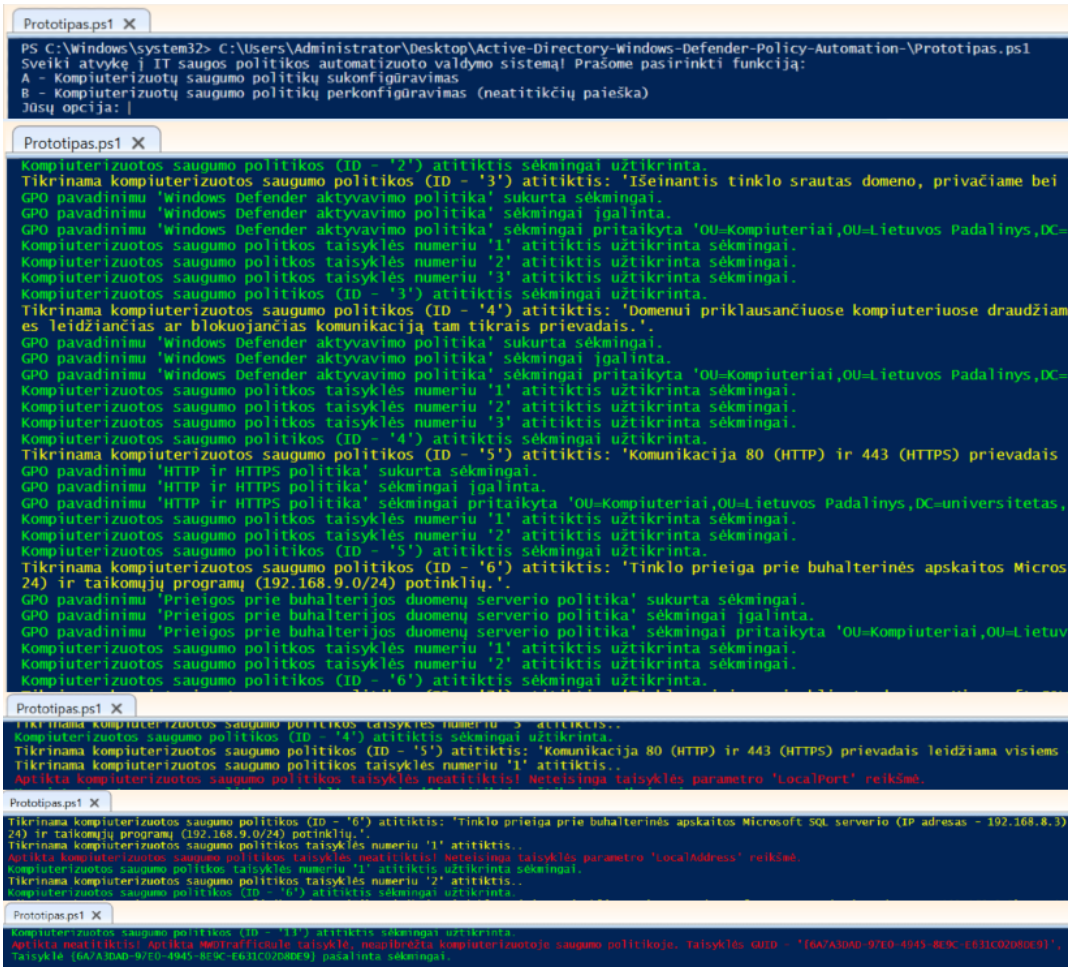


3.20 pav. Pašalinti nereikalingas *MWDTrafficRule* taisykles

Proceso metu naudojamos funkcijos pateiktos priede Nr. 8. Proceso rezultatas – užkirstas kelias KSP neaprašytų *MWDTrafficRule* taisyklių egzistavimui ir ištaisytos *Redundant_MWDTrafficRule* tipo neatitiktys.

3.10. Prototipo terminalinė vartotojo sąsaja

3.21 pav. pavaizduotos ištraukos iš sistemos terminalinės sąsajos.



3.21 pav. Ištraukos iš sistemos terminalinės sąsajos

3.11. Atitikties ataskaita

Sistema užbaigus KSP atitikties tikrinimo procesą sugeneruoja atitikties ataskaitą HTML formatu. Ataskaitoje kiekvieno tipo neatitikčiai yra išskirtas išskleidžiamas lentelės formato sąrašas. Lentelių stulpelių reikšmės priklauso nuo neatitikties objekto atributų, aprašytų 3.4.7 skyriuje. Neatitikties objektų atributų reikšmės atitinka stulpelių pavadinimus. Lentelės eilutės gali būti žalios arba raudonos spalvos, priklausomai nuo „Atitiktis sėkmingai užtikrinta“ reikšmės. Atitikties užtikrinimui pavykus eilutė yra žalios spalvos, nepavykus – raudonos. Dėl išskleidžiamų sąrašų ir lentelių formato ataskaita yra lengvai skaitoma ir suprantama. Ji suteikia aiškią informaciją apie atitikties patikrinimo ir užtikrinimo rezultatus. Svarbu paminėti, kad programos vykdymo pradžioje pasirinkus konfigūravimą nuo pradžių ataskaita nėra generuojama, nes tokiu atveju yra vykdomas sukonfigūravimas pagal KSP, o ne KSP atitikties patikra. Sekančiame skyriuje bus pateikti atitikties ataskaitos pavyzdžiai.

3.12. Išvados

Įgyvendinus sistemos modelio prototipą galima padaryti šias išvadas:

1. Sukurtas prototipas KSP pagalba valdo GP aprašomų registrų reikšmių, ugniasienės profilių ir taisyklių atitiktį.
2. Registrų reikšmių ir ugniasienių profilių ir taisyklių apsirašymas skyriuje pasiūlytu KSP pavidalu yra saugesnis, efektyvesnis ir greitesnis būdas atlikti ugniasienės konfigūravimą ir perkonfigūravimą nei tai būtų daroma rankiniu būdu.
3. Protipo išplečiamumas grindžiamas tuo, kad KSP priklausomai nuo to, kokius parametrus priima KSP nurodytos PowerShell tikrinimo bei užtikrinimo funkcijos, galima pridėti papildomų taisyklės parametrų ir tokiu būdu formuoti tikslesnes, individualius poreikius atitinkančias ugniasienės taisykles.
4. Protipo išplečiamumas grindžiamas tuo, kad KSP formatą galima pritaikyti ir kitų tipų taisyklėms, tereikia programiniame kode apsirašyti funkciją, kuri gebėtų generuoti atitinkamas tikrinimo bei užtikrinimo Poweshell komandas naujo tipo taisyklėms.
5. Prototipo unikalumas pagrindžiamas tuo, kad prototipas geba ne tik aptikti neatitiktis, bet ir jas pašalinti.

4. IT SAUGOS POLITIKOS AUTOMATIZUOTO VALDYMO SISTEMOS TYRIMAS

4.1. Tyrimo planas

Tikslas – ištirti realizuoto prototipo pagrindinių panaudos atvejų rezultatus bei jo veikimo patikimumą. Tyrimui keliami trys pagrindiniai uždaviniai:

- įvertinti prototipo gebėjimą sukonfigūruoti GP pagal KSP;
- įvertinti prototipo gebėjimą aptikti KSP neatitiktis;
- įvertinti prototipo gebėjimą atlikti KSP atitikties užtikrinimą.

4.2. Tyrimo aplinka

4.2.1. Active Directory serverio konfigūracija

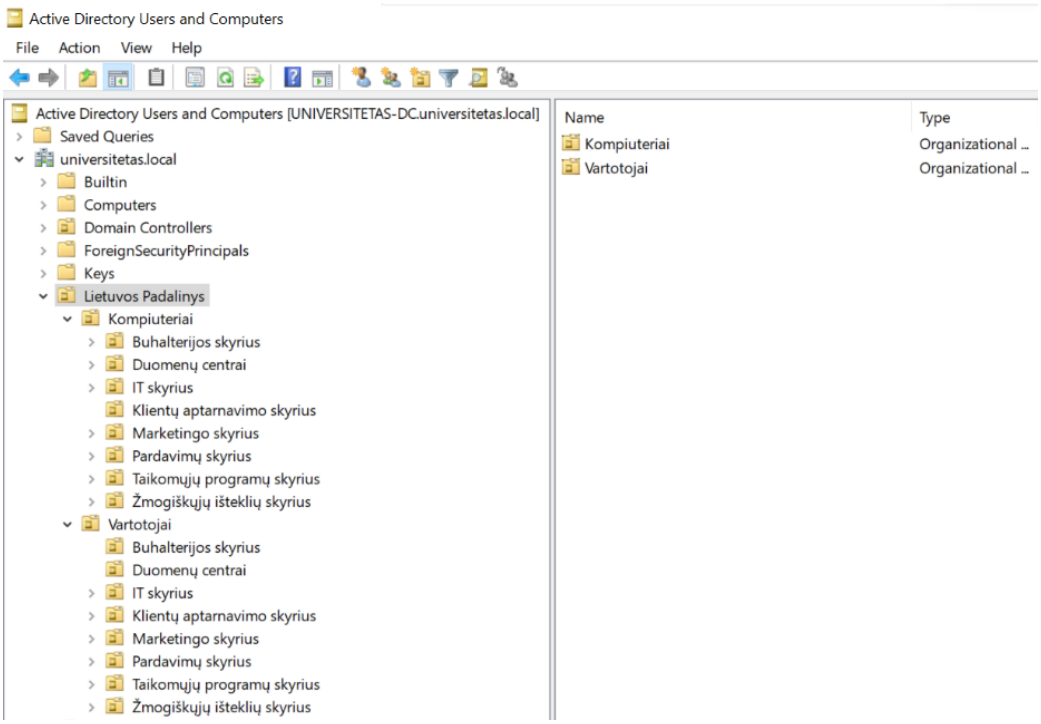
Organizacijos struktūros realizacijai bei sistemos ir KSP testavimui reikalingas Active Directory serveris, 4.1 lentelėje aprašyti serverio konfigūraciniai duomenys.

4.1 lentelė. Active Directory serverio konfigūraciniai duomenys

Parametras	Apibūdinimas
Operacinė sistema	Windows Server 2019
Virtualizacijos platforma	VMware Workstation 17 Player
Serverio ir domeno pavadinimas	UNIVERSITETAS-DC.universitetas.local
Serverio rolės	Active Directory serveris, DNS serveris
Operatyvinė atmintis	4 GB
Procesorius	2 branduoliai
Potinklis	192.168.9.0 / 24
IP adresas	192.168.9.3
Valdymo įrankiai	„Active Directory Users and Computers“ ir „Group Policy Management Console“ programos, PowerShell skriptavimo kalba
Domeno administratorius	akvile.pavardiene@universitetas.local (IT skyrius)

4.2.2. Organizacinės struktūros realizacija Active Directory serveryje

Siekiant ištirti realizuoto prototipo veikimą ir atlikti išsikeltus uždavinius, pirmiausiai reikia realizuoti organizacijos struktūrą – sukurti vartotojų bei kompiuterių OV, taip pat pačius vartotojus bei jų kompiuterius. 4.1 pav. pavaizduota realizuota 2.2 skyrelyje aprašytos organizacijos struktūra.



4.1 pav. Organizacijos infrastruktūra Active Directory serveryje

Organizacijos struktūra skyla į du pagrindinius OV: kompiuterių bei vartotojų. Vartotojų OV realizuoja organizacijos vartotojų paskyras, tuo tarpu kompiuterių OV realizuoja vartotojų kompiuterius.

4.2.3. Organizacijai taikomos kompiuterizuotos saugumo politikos

Organizacijos infrastruktūrai yra taikoma 13 KSP (pateiktos priede Nr. 9), kurios bus naudojamos įgyvendintos IT saugos politikos automatizuoto valdymo sistemos testavimui.

4.3. Sistemos gebėjimo konfigūruoti kompiuterizuotas saugumo politikas kokybinis tyrimas

Tyrimo metu bus ištirtas sistemos gebėjimas atlikti KSP konfigūraciją.

4.3.1. Grupės politikos atsarginės kopijos XML formatu išsaugojimas

Tyrimo metu bus pasitelkta į „Group Policy Management“ programos galimybę išsaugoti GP atsargines kopijas XML formatu, kurių turinyje atsispindi sukonfigūruotos KSP ir jų taisyklės. Norint sugeneruoti GP atsarginę kopiją XML formatu serveryje atsidarius šią programą reikia atlikti žemiau išvardintus žingsnius:

1. Pasirinkti domeną ir išskleisti jo aplanką.
2. Išskleisti *Group Policy Objects* aplanką.
3. Sąraše dešiniuoju pelės klavišu paspausti ant GP.
4. Pasirinkti *Back Up* opciją.

5. Pasirinkti sisteminį kelią, kur bus išsaugota GP atsarginės kopijos aplankas.
6. Išsaugoti aplanką.
7. Pervadinti aplanke esantį gpresult.xml failą į

{GRUPĖS_POLITIKOS_PAVADINIMAS}_SUKONFIGŪRUOTA_RANKINIU_BŪDU arba **{GRUPĖS_POLITIKOS_PAVADINIMAS}_SUKONFIGŪRUOTA_SISTEMOS**, priklausomai nuo to, ar konfigūracija buvo atlikta rankiniu būdu ar sukonfigūruota sistemos.

ATLIKTŲ ŽINGSNIŲ REZULTATAS:

Aplanko viduje bus failas pavadinimu gpresult.xml, kurio turinyje atsispindės GP atlikta konfigūracija. Aktualūs gpresult.xml failo atributai:

- < Identifier>...</Identifier>;
- < Name>...</Name>;
- <CreatedTime>...</CreatedTime>;
- < ModifiedTime>...</ModifiedTime>;
- <ReadTime>...</ReadTime>;
- <Computer>...</Computer>;
- <LinksTo>...</LinksTo>.

4.3.2. Bandymo veiksmų seka

Sistemos gebėjimui sukonfigūruoti GP pagal KSP ištirti reikia atlikti žemiau išvardintus žingsnius:

1. Nuosekliai ir teisingai rankiniu būdu sukonfigūruoti GP pagal KSP naudojant „Group Policy Management“ programą ir įsitikinti, kad konfigūracija yra besąlygiškai teisinga.
2. Išsaugoti kiekvienos rankiniu būdu sukonfigūruotos GP atsarginę kopiją XML formatu pagal 4.3.1 skyrelio nurodymus.
3. Pašalinti visus GP objektus.
4. Sistemos pagalba sukonfigūruoti GP pagal KSP.
5. Išsaugoti kiekvienos sistemos sukonfigūruotos GP atsarginę kopiją XML formatu pagal 4.3.1 skyrelio nurodymus.
6. Palyginti 1 ir 5 žingsnyje sugeneruotų gpresult.xml failų turinius ir nustatyti, ar sistema sukonfigūravo GP taip taip pat kaip ir tai buvo padaryta rankiniu būdu.
7. Pakomentuoti nesutapimus (jei jų yra) ir jų priežastis, kodėl jie galėjo atsirasti.

PASTABA: {GRUPĖS_POLITIKOS_PAVADINIMAS}_SUKONFIGŪRUOTA_RANKINIU_BŪDU ir **{GRUPĖS_POLITIKOS_PAVADINIMAS}_SUKONFIGŪRUOTA_SISTEMOS** failai bandyme bus vadinamas išvesties failais.

REKOMENDACIJA: siekiant padaryti išvesties failus lengviau skaitomais iš jų pašalinti nereikalingus, tyrimo rezultatui įtakos neturinčius atributus.

4.3.3. Bandymas

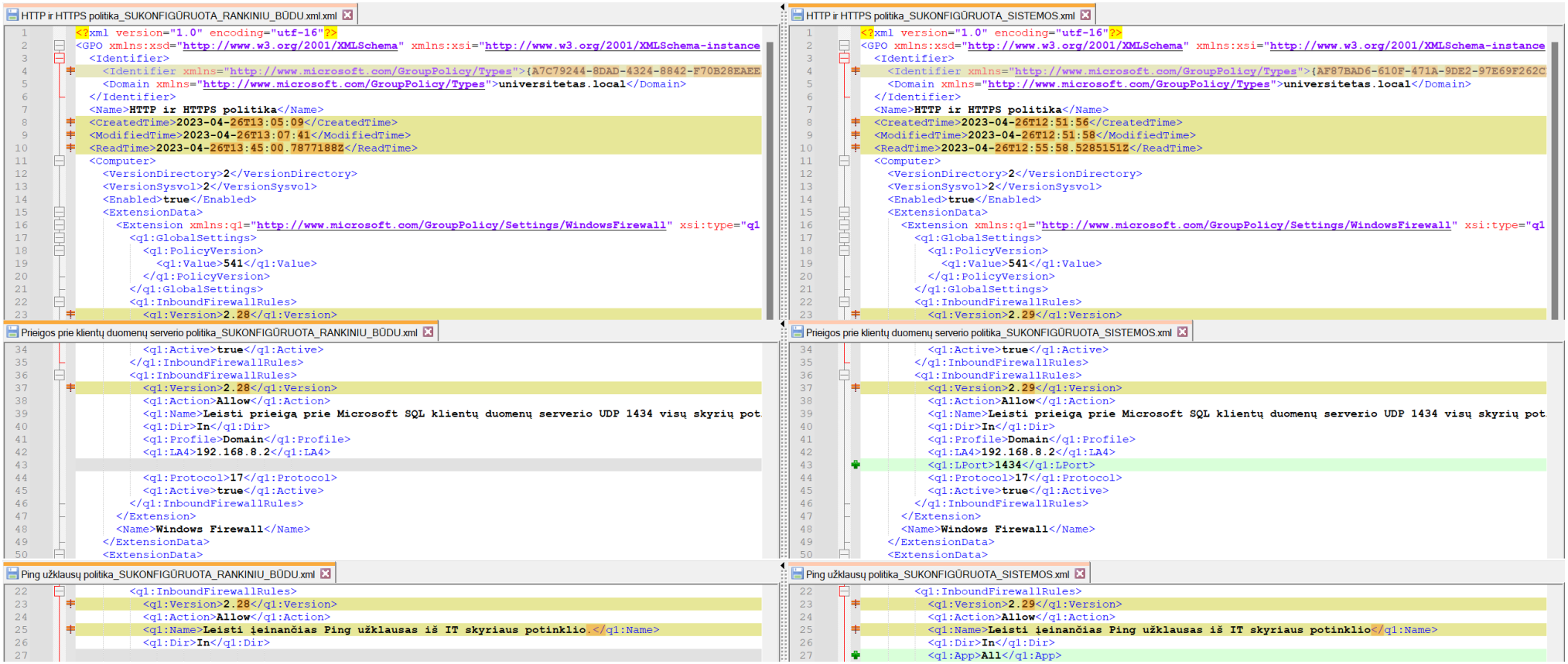
Bandymo metu rankiniu būdu buvo atlikta universitetas.local GP konfigūracija pagal KSP vadovaujantis sistemos programinio kodo logika. 4.2 lentelėje pavaizduoti bandymo rezultatai.

Pirmame ir antrajame stulpeliuose matosi GP, kurių konfigūracija buvo atliekama pagal KSP aprašytas taisykles, atsarginių kopijų XML formatu pavadinimai po pervadinimo pagal 4.3.1 pateiktus žingsnius. Trečiajame stulpelyje matoma failų turinio sutapties procentinė dalis.

4.2 lentelė. Konfigūravimo bandymo rezultatai

Išvesties failo pavadinimas po rankinio konfigūravimo	Išvesties failo pavadinimas po sistemos atlikto konfigūravimo	Failų sutaptis
Windows Defender aktyvavimo politika_SUKONFIGŪRUOTA_RANKINIU_BŪDU.xml	Windows Defender aktyvavimo politika_SUKONFIGŪRUOTA_SISTEMOS.xml	99.66 %
HTTP ir HTTPS politika_SUKONFIGŪRUOTA_RANKINIU_BŪDU.xml	HTTP ir HTTPS politika_SUKONFIGŪRUOTA_SISTEMOS.xml	96.59 %
Prieigos prie buhalterijos duomenų serverio politika_SUKONFIGŪRUOTA_RANKINIU_BŪDU.xml	Prieigos prie buhalterijos duomenų serverio politika_SUKONFIGŪRUOTA_SISTEMOS.xml	98.42 %
Prieigos prie klientų duomenų serverio politika_SUKONFIGŪRUOTA_RANKINIU_BŪDU.xml	Prieigos prie klientų duomenų serverio politika_SUKONFIGŪRUOTA_SISTEMOS.xml	97.36 %
Prieigos prie Microsoft Dynamics Nav Web serverio politika_SUKONFIGŪRUOTA_RANKINIU_BŪDU.xml	Prieigos prie Microsoft Dynamics Nav Web serverio politika_SUKONFIGŪRUOTA_SISTEMOS.xml	98.10 %
RDP politika_SUKONFIGŪRUOTA_RANKINIU_BŪDU.xml	RDP politika_SUKONFIGŪRUOTA_SISTEMOS.xml	97.59 %
Ping užklausų politika_SUKONFIGŪRUOTA_RANKINIU_BŪDU.xml	Ping užklausų politika_ SUKONFIGŪRUOTA_SISTEMOS.xml	95.08 %
RDP įgalinimo politika_SUKONFIGŪRUOTA_RANKINIU_BŪDU.xml	RDP įgalinimo politika_ SUKONFIGŪRUOTA_SISTEMOS.xml	97.77 %
Tinklo lygio autentifikacijos politika_SUKONFIGŪRUOTA_RANKINIU_BŪDU.xml	Tinklo lygio autentifikacijos politika_ SUKONFIGŪRUOTA_SISTEMOS.xml	98.37 %
Spausdintuvo naudojimo politika_SUKONFIGŪRUOTA_RANKINIU_BŪDU.xml	Spausdintuvo naudojimo politika_SUKONFIGŪRUOTA_SISTEMOS.xml	99.36 %

Remiantis lentelėje pateiktais bandymo rezultatais matoma, kad failų sutapčių procentinės dalys svyruoja nuo 95.08 % iki 99.36 %. Tyrimo vykdymo metu pastebėta, kad konfigūruojant rankiniu būdu buvo padaryta viena stambi ir kelios smulkios klaidos kelių ugniasienės taisyklių konfigūracijoje (gramatinės klaidos ugniasienės taisyklių pavadinimuose), tačiau likusi dalis nesutapimų iš esmės buvo *Identifier* (GP unikalus identifikatorius), *CreatedTime* (GP sukūrimo laikas), *ModifiedTime* (GP parametrų keitimo laikas), *ReadTime* (GP peržiūrėjimo laikas) reikšmių nesutapimai, kurie yra visiškai nereikšmingi ir neturintys įtakos tyrimo išvadoms. 4.2 pav. pavaizduotos ištraukos iš kelių išvesties failų portų sutapties patikrinimo.



4.2 pav. Išvesties failų sutaptys

Paveikslėlio vidurinėje sutaptyje kairėje ir dešinėje esančiose 43 eilutėse matomas skirtumas. Rankinio konfigūravimo metu buvo nenustatytas vienas iš svarbiausių ugniasienės taisyklės parametrų – *LPort* (*LocalPort*), tačiau sistemos atlikto konfigūravimo metu jo reikšmė (1434) buvo nustatyta. Tai reiškia, kad bandymo metu įvyko žmogiškoji klaida ir šiuo atveju konfigūracija atlikta sistemos, priešingai nei rankiniu būdu, yra teisinga. Tai tik dar kartą patvirtina būtinybę automatizuoti ugniasienės taisyklių kūrimą, nes ilgi, kruopštumo ir susikaupimo reikalaujantys konfigūracijos darbai neretai nulemia žmogiškųjų klaidų atsiradimą. Apibendrinant galima teigti, kad sistema sukonfigūruoja GP taip pat kaip ir tai atliekama rankiniu būdu (su sąlyga, kad neįvyksta žmogiškųjų klaidų). Skirtumas tik tame, kad konfigūracija sistemos pagalba reikalauja žymiai mažiau laiko ir pastangų.

4.4. Sistemos gebėjimo tikrinti ir užtikrinti kompiuterizuotos saugumo politikos atitiktį kokybinis tyrimas

Tyrimo bandymų metu bus ištirtas sistemos gebėjimas aptikti ir ištaisyti KSP taisyklių neatitiktis.

4.4.1. Bandymų veiksmų seka

Kiekvieno bandymo metu reikia atlikti šiuos žingsnius:

1. Sistemos pagalba sukonfigūruoti GP pagal KSP.
2. Rankiniu būdu tyčia inicijuoti pasirinktų KSP taisyklių neatitiktis (prie kiekvieno bandymo pridėti tyčia inicijuotų neatitikčių lentelę).
3. Sistemos pagalba atlikti KSP neatitikčių paiešką (prie kiekvieno bandymo pateikti bandymo metu sugeneruotą atitikties ataskaitą).
4. Kiekvieno bandymo pabaigoje pakomentuoti apie tyčia inicijuotų ir aptiktų neatitikčių poras.
5. Pakartotinai sistemos pagalba atlikti KSP neatitikčių paiešką.

ATLIKTŲ ŽINGSNIŲ TIKĖTINAS REZULTATAS:

3. Sugeneruota atitikties ataskaita, kurioje atsispindi antrajame žingsnyje rankiniu būdu tyčia inicijuotos neatitiktys.

5. Sugeneruota tuščia atitikties ataskaita. Sistemai veikiant korektiškai trečiajame žingsnyje neatitiktys turėjo būti ištaisytos, todėl pakartotinai inicijavus neatitikčių paiešką jos neturi būti aptinkamos.

PASTABA:

Sistemai neaptikus tyčia rankiniu būdu inicijuotos neatitikties (-čių) pakomentuoti, kas galėjo padaryti įtaką tam, jog ji nebuvo aptikta.

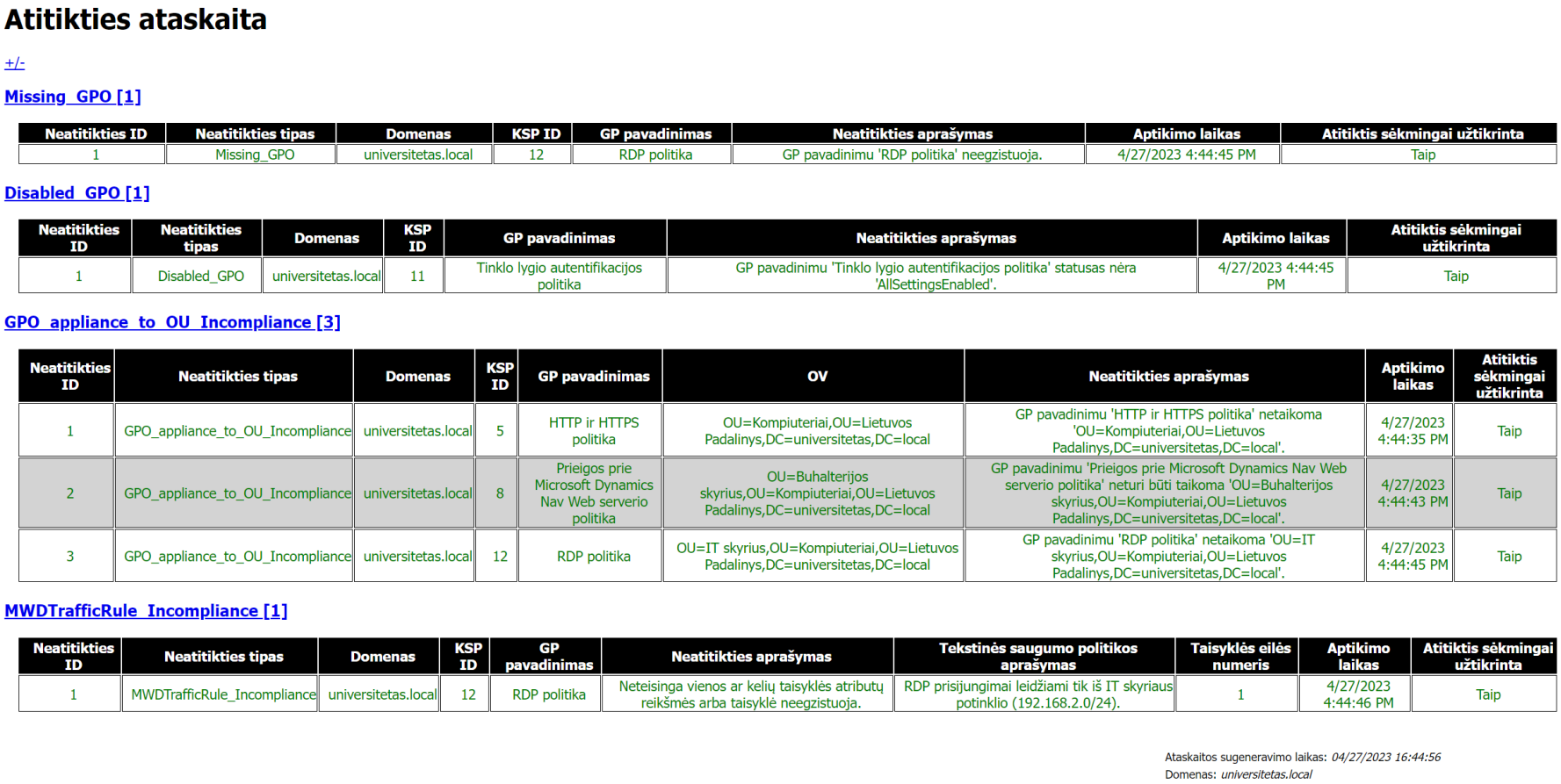
4.4.2. Bandymas Nr. 1

Bandymo metu bus ištirtas sistemos gebėjimas aptikti *Missing_GPO*, *Disabled_GPO* bei *GPO_appliance_to_OU_Incompliance* tipų neatitiktis ir jas atpažinus perkonfigūruoti GP pagal KSP. 4.3 lentelėje pavaizduoti tyčia inicijuoti KSP pažeidimai.

4.3 lentelė. *Missing_GPO, Disabled_GPO, GPO_appliance_to_OU_Incompliance* neatitiktys

KSP ID	Neatitikties tipas	Neatitikties paaiškinimas
12	*Missing_GPO*	KSP (ID = 12), GroupPolicyName reikšmėje nurodytu pavadinimu GP neegzistuoja.
11	*Disabled_GPO*	KSP (ID = 11), GroupPolicyName reikšmėje nurodytu pavadinimu GP yra neįgalinta.
8	*GPO_appliance_to_OU _Incompliance*	KSP (ID = 8), GroupPolicyName reikšmėje nurodytu pavadinimu GP yra taikoma **OU = Buhalterijos skyrius, OU = Kompiuteriai, OU = Lietuvos Padalinys, DC = universitetas, DC=local**, nors pagal KSP šiam OV ji neturi būti taikoma.
5	*GPO_appliance_to_OU _Incompliance*	KSP (ID = 5), GroupPolicyName reikšmėje nurodytu pavadinimu GP netaikoma **OU = Kompiuteriai, OU = Lietuvos Padalinys, DC = universitetas, DC = local**, nors pagal KSP šiam OV ji turi būti taikoma.

Inicijavus lentelėje pateiktas neatitiktis buvo paleista sistema, kuri GP konfigūracijoje ieškojo neatitikčių. Patikros rezultatai pavaizduoti 4.3 pav.



Atitikties ataskaita

+/-

Missing_GPO [1]

Neatitikties ID	Neatitikties tipas	Domenas	KSP ID	GP pavadinimas	Neatitikties aprašymas	Aptikimo laikas	Atitiktis sėkmingai užtikrinta
1	Missing_GPO	universitetas.local	12	RDP politika	GP pavadinimu 'RDP politika' neegzistuoja.	4/27/2023 4:44:45 PM	Taip

Disabled_GPO [1]

Neatitikties ID	Neatitikties tipas	Domenas	KSP ID	GP pavadinimas	Neatitikties aprašymas	Aptikimo laikas	Atitiktis sėkmingai užtikrinta
1	Disabled_GPO	universitetas.local	11	Tinklo lygio autentifikacijos politika	GP pavadinimu 'Tinklo lygio autentifikacijos politika' statusas nėra 'AllSettingsEnabled'.	4/27/2023 4:44:45 PM	Taip

GPO_appliance_to_OU_Incompliance [3]

Neatitikties ID	Neatitikties tipas	Domenas	KSP ID	GP pavadinimas	OV	Neatitikties aprašymas	Aptikimo laikas	Atitiktis sėkmingai užtikrinta
1	GPO_appliance_to_OU_Incompliance	universitetas.local	5	HTTP ir HTTPS politika	OU=Kompiuteriai,OU=Lietuvos Padalinys,DC=universitetas,DC=local	GP pavadinimu 'HTTP ir HTTPS politika' netaikoma 'OU=Kompiuteriai,OU=Lietuvos Padalinys,DC=universitetas,DC=local'.	4/27/2023 4:44:35 PM	Taip
2	GPO_appliance_to_OU_Incompliance	universitetas.local	8	Prieigos prie Microsoft Dynamics Nav Web serverio politika	OU=Buhalterijos skyrius,OU=Kompiuteriai,OU=Lietuvos Padalinys,DC=universitetas,DC=local	GP pavadinimu 'Prieigos prie Microsoft Dynamics Nav Web serverio politika' neturi būti taikoma 'OU=Buhalterijos skyrius,OU=Kompiuteriai,OU=Lietuvos Padalinys,DC=universitetas,DC=local'.	4/27/2023 4:44:43 PM	Taip
3	GPO_appliance_to_OU_Incompliance	universitetas.local	12	RDP politika	OU=IT skyrius,OU=Kompiuteriai,OU=Lietuvos Padalinys,DC=universitetas,DC=local	GP pavadinimu 'RDP politika' netaikoma 'OU=IT skyrius,OU=Kompiuteriai,OU=Lietuvos Padalinys,DC=universitetas,DC=local'.	4/27/2023 4:44:45 PM	Taip

MWDTrafficRule_Incompliance [1]

Neatitikties ID	Neatitikties tipas	Domenas	KSP ID	GP pavadinimas	Neatitikties aprašymas	Tekstinės saugumo politikos aprašymas	Taisyklės eilės numeris	Aptikimo laikas	Atitiktis sėkmingai užtikrinta
1	MWDTrafficRule_Incompliance	universitetas.local	12	RDP politika	Neteisinga vienos ar kelių taisyklės atributų reikšmės arba taisyklė neegzistuoja.	RDP prisijungimai leidžiami tik iš IT skyriaus potinklio (192.168.2.0/24).	1	4/27/2023 4:44:46 PM	Taip

Ataskaitos sugeneravimo laikas: *04/27/2023 16:44:56*
Domenas: *universitetas.local*

4.3 pav. Bandymo Nr. 1 ataskaita

Iš sugeneruotos ataskaitos matyti, kad buvo aptiktos visos lentelėje aprašytos tyčia inicijuotos neatitiktys. Pastebėta, kad pirmoji *Missing_GPO* neatitiktis padarė įtaką tam, kad buvo paleistos papildomos užtikrinimo veiksmų sekos: GP priskyrimo OV (*GPO_appliance_to_OU_Incompliance* trečioji neatitiktis) ir ugniasienės taisyklės sukūrimo (*MWDTrafficRule_Incompliance* pirmoji neatitiktis). Tai yra rezultatas, kurio ir tikimasi iš sistemos. Kadangi GP neegzistuoja, ji nėra priskirta reikiamam OV, taip pat ir neegzistuoja joje aprašytos ugniasienės ir kitos taisyklės, tai sistema laiko neatitiktimis, kurias reikia ištaisyti, ką sistema ir padarė. Tęsiant bandymą ir pakartotinai paleidus neatitikčių nebeaptiko, o tai patvirtina, kad užtikrinimo veiksmų sekos buvo sėkmingai paleistos ir įvykdytos.

4.4.3. Bandymas Nr. 2

Bandymo metu bus ištirtas sistemos gebėjimas aptikti ir ištaisyti *ADMXRule_Incompliance* tipo neatitiktis. Apačioje 4.4 lentelėje pavaizduoti tyčia inicijuoti KSP taisyklių pažeidimai.

4.4 lentelė. *ADMXRule_Incompliance* neatitiktys

KSP ID	Taisyklės eilės numeris	Registras	Klaidinga registro reikšmė	Teisinga registro reikšmė
1	1	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\ WindowsFirewall\DomainProfile\EnableFirewall	Value = 0	Value = 1
10	1	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\ Windows NT\Terminal Services\fDenyTSConnections	Value = 1	Value = 0
11	1	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\ Windows NT\Terminal Services\UserAuthentication	Value = 0	Value = 1

Inicijavus lentelėje pateiktas neatitiktis buvo paleista sistema, kuri GP konfigūracijoje ieškojo neatitikčių. Patikros rezultatai pavaizduoti 4.4 pav.

Atitikties ataskaita

+/-

ADMXRule_Incompliance [3]

Neatitikties ID	Neatitikties tipas	Domenas	KSP ID	GP pavadinimas	Neatitikties aprašymas	Tekstinės saugumo politikos aprašymas	Taisyklės eilės numeris	Aptikimo laikas	Atitiktis sėkmingai užtikrinta
1	ADMXRule_Incompliance	universitetas.local	1	Windows Defender aktyvavimo politika	Neteisinga registro 'HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\EnableFirewall' reikšmė	Windows Defender ugniasienė turi būti aktyvuota domeno, privačiame ir viešajame tinklo profiliuose.	1	4/28/2023 1:06:14 PM	Taip
2	ADMXRule_Incompliance	universitetas.local	10	RDP įgalinimo politika	Neteisinga registro 'HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\fDenyTSConnections' reikšmė	RDP prisijungimai turi būti įgalinti visuose organizacijos kompiuteriuose.	1	4/28/2023 1:06:39 PM	Taip
3	ADMXRule_Incompliance	universitetas.local	11	Tinklo lygio autentifikacijos politika	Neteisinga registro 'HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\UserAuthentication' reikšmė	Tinklo lygio autentifikacija turi būti įgalinta visuose organizacijos kompiuteriuose.	1	4/28/2023 1:06:40 PM	Taip

Ataskaitos sugeneravimo laikas: *04/28/2023 13:06:52*
Domenas: *universitetas.local*

4.4 pav. Bandymo Nr. 2 ataskaita

Iš sugeneruotos ataskaitos matyti, kad buvo aptiktos visos lentelėje aprašytos tyčia inicijuotos neatitiktys. Neatitikties aprašymo stulpelyje įvardinti registrai, kurių reikšmės sukonfigūruotos klaidingai. Taip pat iš atitikties ataskaitos matyti, kad visos neatitiktys buvo sėkmingai pašalintos. Iš bandymo rezultatų galima daryti išvadą, kad sistema geba tiek aptikti, tiek ištaisyti *ADMXRule_Incompliance* tipo neatitiktis. Tęsiant bandymą ir pakartotinai paleidus neatitikčių nebeaptiko, o tai patvirtina, kad užtikrinimo veiksmų sekos buvo sėkmingai paleistos ir įvykdytos.

4.4.4. Bandymas Nr. 3

Bandymo metu bus ištirtas sistemos gebėjimas apdoroti *MWDProfileRule_Incompliance* tipo neatitiktis. Bandymo tikslas yra pademonstruoti sistemos gebėjimą atpažinti klaidingą tinklo profilių konfigūraciją ir ją atpažinus perkonfigūruoti pagal KSP. 4.5 lentelėje pavaizduoti tyčia inicijuoti KSP taisyklių pažeidimai.

4.5 lentelė. *MWDProfileRule_Incompliance* neatitiktys

KSP ID	Taisyklės eilės numeris	Klaidinga atributo reikšmė	Teisinga atributo reikšmė
2	1	DefaultInboundAction = Allow	DefaultInboundAction = Block
3	1	DefaultOutboundAction = Block	DefaultOutboundAction = Allow
4	2	AllowUserApps = True	AllowUserApps = False
4	2	AllowLocalFirewallRules = True	AllowLocalFirewallRules = False
4	3	AllowUserPorts = True	AllowUserPorts = False

Inicijavus lentelėje pateiktas neatitiktis buvo paleista sistema, kuri GP konfigūracijoje ieškojo neatitikčių. Patikros rezultatai pavaizduoti 4.5 pav.

Atitikties ataskaita

+/-

MWDProfileRule_Incompliance [4]

Neatitikties ID	Neatitikties tipas	Domenas	KSP IP	GP pavadinimas	Neatitikties aprašymas	Tekstinės saugumo politikos aprašymas	Taisyklės eilės numeris	Aptikimo laikas	Atitiktis sėkmingai užtikrinta
1	MWDProfileRule_Incompliance	universitetas.local	2	Windows Defender aktyvavimo politika	Neteisinga parametro 'DefaultInboundAction' reikšmė 'Domain' profilyje	Įeinantis tinklo srautas domeno, privačiame bei viešajame tinklo profiliuose, neatitinkantis grupės politikose aprašytų Windows Defender ugniasienės taisyklių turi būti blokuojamas.	1	4/30/2023 2:33:47 PM	Taip
2	MWDProfileRule_Incompliance	universitetas.local	3	Windows Defender aktyvavimo politika	Neteisinga parametro 'DefaultOutboundAction' reikšmė 'Domain' profilyje	Išeinantis tinklo srautas domeno, privačiame bei viešajame tinklo profiliuose, neatitinkantis grupės politikose aprašytų Windows Defender ugniasienės taisyklių yra leidžiamas.	1	4/30/2023 2:33:59 PM	Taip
3	MWDProfileRule_Incompliance	universitetas.local	4	Windows Defender aktyvavimo politika	Neteisinga parametro 'AllowLocalFirewallRules' reikšmė 'Private' profilyje	Domenui priklausančiuose kompiuteriuose draudžiama diegti programinę įrangą, kuri nėra leidžiama grupės politikos taisyklių, taip pat draudžiama manipuliuoti prievadų būsena, t.y kurti ugniasienės taisykles leidžiančias ar blokuojančias komunikaciją tam tikrais prievadais.	2	4/30/2023 2:34:10 PM	Taip
4	MWDProfileRule_Incompliance	universitetas.local	4	Windows Defender aktyvavimo politika	Neteisinga parametro 'AllowUserPorts' reikšmė 'Public' profilyje	Domenui priklausančiuose kompiuteriuose draudžiama diegti programinę įrangą, kuri nėra leidžiama grupės politikos taisyklių, taip pat draudžiama manipuliuoti prievadų būsena, t.y kurti ugniasienės taisykles leidžiančias ar blokuojančias komunikaciją tam tikrais prievadais.	3	4/30/2023 2:34:16 PM	Taip

Ataskaitos sugeneravimo laikas: *04/30/2023 14:34:17*
Domenas: *universitetas.local*

4.5 pav. Bandymo Nr. 3 ataskaita

Iš sugeneruotos ataskaitos matyti, kad buvo aptiktos ne visos lentelėje aprašytos tyčia inicijuotos neatitiktys. 4.5 lentelėje aprašyta tyčia inicijuota neatitiktis (KSP ID - 4, o taisyklės eilės numeris - 2) nurodanti, kad *AllowUserApps* reikšmė yra *True*, nebuvo aptikta. Tačiau tai yra rezultatas, kurio ir tikimasi iš sistemos. Šioje taisyklėje tyčia buvo inicijuotos dvi neatitiktys, o taisyklėje aptikus daugiau nei vieną neatitiktį po pirmosios aptikimo yra perkonfigūruojama visa taisyklė, o kiti taisyklės atributai toliau nėra tikrinami. Šioje taisyklėje pirmiausiai buvo aptikta neteisinga atributo *AllowLocalFirewallRules* reikšmė, ko pasekoje iškart buvo perkonfigūruota visa taisyklė, todėl neteisinga *AllowUserApps* atributo reikšmė nebuvo aptikta. Dėl šios priežasties 4.5 lentelėje pavaizduoda neatitiktis (KSP ID - 4, o taisyklės eilės numeris - 3), nurodanti, kad *AllowUserApps* reikšmė yra klaidinga (*True*), nebuvo aptikta. Iš bandymo rezultatų galima daryti išvadą, kad sistema geba tiek aptikti, tiek ištaisyti *MWDProfileRule_Incompliance* tipo neatitiktis. Tęsiant bandymą ir pakartotinai paleidus neatitikčių nebeaptiko, o tai patvirtina, kad užtikrinimo veiksmų sekos buvo sėkmingai paleistos ir įvykdytos.

4.4.5. Bandymas Nr. 4

Bandymo metu bus ištirtas sistemos gebėjimas aptikti ir ištaisyti *MWDTrafficRule_Incompliance* tipo neatitiktis. Imituojant žmogiškųjų klaidų atsiradimą bus sugadinama tam tikrų ugniasienės taisyklių konfigūracija ir bus tikrinama, ar sistema geba aptikti ir ištaisyti klaidingą ugniasienės konfigūraciją. 4.6 lentelėje pavaizduoti tyčia inicijuoti KSP taisyklių pažeidimai.

4.6 lentelė. *MWDTrafficRule_Incompliance* neatitiktys

KSP ID	Taisyklės eilės numeris	Klaidinga parametro reikšmė	Teisinga parametro reikšmė
5	2	Action = Block	Action = Allow
6	2	LocalAddress = 192.168.8.2	LocalAddress = 192.168.8.3
7	1	LocalPorts = 1434, 4022	LocalPorts = 1433, 1434, 4022, 135
8	1	LocalPorts = 80, 4443	LocalPorts = 80, 443
9	1	RemoteAddress = 192.168.4.0/255.255.255.0	RemoteAddress = 192.168.2.0/255.255.255.0
12	1	Protocol = UDP	Protocol = TCP
13	3	Profile = Private	Profile = Domain

Inicijavus lentelėje pateiktas neatitiktis buvo paleista sistema, kuri GP konfigūracijoje ieškojo neatitikčių. Patikros rezultatai pavaizduoti 4.6 pav.

Atitikties ataskaita

+/-

MWDTrafficRule_Incompliance [7]

Neatitikties ID	Neatitikties tipas	Domenas	KSP IP	GP pavadinimas	Neatitikties aprašymas	Tekstinės saugumo politikos aprašymas	Taisyklės eilės numeris	Aptikimo laikas	Atitiktis sėkmingai užtikrinta
1	MWDTrafficRule_Incompliance	universitetas.local	5	HTTP ir HTTPS politika	Neteisinga taisyklės parametro 'Action' reikšmė.	Komunikacija 80 (HTTP) ir 443 (HTTPS) prievadais leidžiama visiems domeno Lietuvos padalinio kompiuteriams.	2	5/2/2023 12:07:42 PM	Taip
2	MWDTrafficRule_Incompliance	universitetas.local	6	Prieigos prie buhalterijos duomenų serverio politika	Neteisinga taisyklės parametro 'LocalAddress' reikšmė.	Tinklo prieiga prie buhalterinės apskaitos Microsoft SQL serverio (IP adresas - 192.168.8.3) TCP 1433, 1434, 4022, 135 ir UDP 1434 prievadų leidžiama tik iš buhalterijos (192.168.7.0/24), IT (192.168.2.0/24) ir taikomųjų programų (192.168.9.0/24) potinklių.	2	5/2/2023 12:07:49 PM	Taip
3	MWDTrafficRule_Incompliance	universitetas.local	7	Prieigos prie klientų duomenų serverio politika	Neteisinga taisyklės parametro 'LocalPort' reikšmė.	Tinklo prieiga prie klientų duomenų Microsoft SQL serverio (IP adresas - 192.168.8.2) TCP 1433, 1434, 4022, 135 ir UDP 1434 prievadų leidžiama iš visų skyrių potinklių.	1	5/2/2023 12:07:55 PM	Taip
4	MWDTrafficRule_Incompliance	universitetas.local	8	Prieigos prie Microsoft Dynamics Nav Web serverio politika	Neteisinga taisyklės parametro 'LocalPort' reikšmė.	Tinklo prieiga prie Microsoft Dynamics Nav Web serverio (IP adresas - 192.168.9.2) TCP 80, 443 prievadų leidžiama visiems skyrių potinkliams išskyrus žmogiškųjų išteklių skyriaus potinkliui.	1	5/2/2023 12:07:58 PM	Taip
5	MWDTrafficRule_Incompliance	universitetas.local	9	Ping užklausų politika	Neteisinga taisyklės parametro 'RemoteAddress' reikšmė.	Ping užklausos yra leidžiamos tik iš IT skyriaus potinklio (192.168.2.0/24).	1	5/2/2023 12:08:02 PM	Taip
6	MWDTrafficRule_Incompliance	universitetas.local	12	RDP politika	Neteisinga taisyklės parametro 'Protocol' reikšmė.	RDP prisijungimai leidžiami tik iš IT skyriaus potinklio (192.168.2.0/24).	1	5/2/2023 12:08:09 PM	Taip
7	MWDTrafficRule_Incompliance	universitetas.local	13	Spausdintuvo naudojimo politika	Neteisinga taisyklės parametro 'Profile' reikšmė.	Tinklo prieiga prie nutolusio spausdintuvo leidžiama tik iš IT (192.168.2.0/24), žmogiškųjų išteklių (192.168.3.0/24), marketingo (192.168.4.0/24) , klientų aptarnavimo (192.168.5.0/24), pardavimų (192.168.6.0/24), buhalterijos (192.168.7.0/24) skyrių potinklių.	3	5/2/2023 12:08:16 PM	Taip

Ataskaitos sugeneravimo laikas: *05/02/2023 12:08:23*
Domenas: *universitetas.local*

4.6 pav. Bandymo Nr. 4 ataskaita

Iš sugeneruotos ataskaitos matyti, kad buvo aptiktos visos lentelėje aprašytos tyčia inicijuotos neatitiktys. Matoma, kad sistema geba ne tik nustatyti ugniasienės taisyklės pažeidimo faktą, tačiau ir pateikti informaciją apie tai, kokio ugniasienės taisyklės parametro reikšmė yra neteisinga. Iš bandymo rezultatų galima daryti išvadą, kad sistema geba tiek aptikti, tiek ištaisyti *MWDTrafficRule_Incompliance* tipo neatitiktis. Tęsiant bandymą ir pakartotinai paleidus neatitikčių nebeaptiko, o tai patvirtina, kad užtikrinimo veiksmų sekos buvo sėkmingai paleistos ir įvykdytos.

4.4.6. Bandymas Nr. 5

Bandymo metu bus ištirtas sistemos gebėjimas aptikti ir ištaisyti *Redundant_MWDTrafficRule* tipo neatitiktis. Bandymo tikslas yra pademonstruoti sistemos gebėjimą atpažinti ir pašalinti KSP neaprašytas ugniasienės taisykles. Daroma prielaida, kad 4.7 lentelėje aprašytos taisyklės atsirado dėl žmogiškųjų klaidų ir rankinio konfigūravimo metu buvo sukurtos netyčia.

4.7 lentelė. *Redundant_MWDTrafficRule* neatitiktys

KSP ID	GP pavadinimas	Perteklinės ugniasienės taisyklės apibrėžimas
5	HTTP ir HTTPS politika	• DisplayName: "Leisti įeinantį HTTP srautą" • Direction: Inbound • Protocol: UDP • LocalAddress: Any • RemoteAddress: Any • LocalPort: 80 • RemotePort: Any • Action: Allow
6	Prieigos prie buhalterijos duomenų serverio politika	• DisplayName: Leisti prieigą prie Microsoft SQL klientų duomenų serverio UDP 1433 visų skyrių potinkliams. • Direction: Inbound • Protocol: UDP • LocalAddress: 192.168.8.2 • RemoteAddress: Any • LocalPort: 1433 • RemotePort: Any • Action: Allow
8	Prieigos prie Microsoft Dynamics Nav Web serverio politika	• DisplayName: Blokuoti prieigą prie Microsoft Dynamics Nav Web serverio TCP 80, 443 prievadų žmogiškųjų išteklių skyriui. • Direction: Inbound • Protocol: TCP • LocalAddress: Any • RemoteAddress: Any • LocalPort: Any • RemotePort: Any • Action: Allow
12	RDP politika	• DisplayName: Leisti RDP sujungimus tik iš IT skyriaus potinklio. • Direction: Outbound • Protocol: TCP • LocalAddress: Any • RemoteAddress: Any • LocalPort: 3389 • RemotePort: Any • Action: Block

Inicijavus lentelėje pateiktas neatitiktis buvo paleista sistema, kuri GP konfigūracijoje ieškojo neatitikčių. Patikros rezultatai pavaizduoti 4.7 pav.

Atitikties ataskaita

+/-

Redundant_MWDTrafficRule_Incompliance [4]

Neatitikties ID	Neatitikties tipas	Domenas	GP pavadinimas	Neatitikties aprašymas	Taisyklės GUID	Taisyklės pavadinimas	Aptikimo laikas	Atitiktis sėkmingai užtikrinta
1	Redundant_MWDTrafficRule_Incompliance	universitetas.local	HTTP ir HTTPS politika	Aptikta MWDTrafficRule taisyklė, neapibrėžta kompiuterizuotoje saugumo politikoje.	{4c88aa76-8d8b-4202-af31-66dd18973943}	Leisti įeinantį HTTP srautą	5/1/2023 12:31:29 AM	Taip
2	Redundant_MWDTrafficRule_Incompliance	universitetas.local	Prieigos prie buhalterijos duomenų serverio politika	Aptikta MWDTrafficRule taisyklė, neapibrėžta kompiuterizuotoje saugumo politikoje.	{61c44e77-9599-4e01-8284-5b1f64384ab5}	Leisti prieigą prie Microsoft SQL klientų duomenų serverio UDP 1433 visų skyrių potinkliams.	5/1/2023 12:31:30 AM	Taip
3	Redundant_MWDTrafficRule_Incompliance	universitetas.local	Prieigos prie Microsoft Dynamics Nav Web serverio politika	Aptikta MWDTrafficRule taisyklė, neapibrėžta kompiuterizuotoje saugumo politikoje.	{0b970dd6-b505-45e8-87d8-56ea5d8290a6}	Blokuoti prieigą prie Microsoft Dynamics Nav Web serverio TCP 80, 443 prievadų žmogiškųjų išteklių skyriui.	5/1/2023 12:31:31 AM	Taip
4	Redundant_MWDTrafficRule_Incompliance	universitetas.local	RDP politika	Aptikta MWDTrafficRule taisyklė, neapibrėžta kompiuterizuotoje saugumo politikoje.	{a45c8732-10cd-449f-873c-169095eebff1}	Leisti RDP sujungimus tik iš IT skyriaus potinklio	5/1/2023 12:31:32 AM	Taip

Ataskaitos sugeneravimo laikas: *05/01/2023 00:31:32*
Domenas: *universitetas.local*

4.7 pav. Bandymo Nr. 5 ataskaita

Iš sugeneruotos ataskaitos matyti, kad buvo aptiktos visos lentelėje aprašytos tyčia inicijuotos neatitiktys. Paskutinis lentelės stulpelis nurodo, kad visos neatitiktys yra sėkmingai pašalintos, o tai reiškia tai, kad visos perteklinės ugniasienės taisyklės buvo aptiktos ir sėkmingai pašalintos iš atitinkamų GP. Iš bandymo rezultatų galima daryti išvadą, kad sistema geba tiek aptikti, tiek ištaisyti *Redundant_MWDTrafficRule* tipo neatitiktis. Tęsiant bandymą ir pakartotinai paleidus neatitikčių nebeaptiko, o tai patvirtina, kad užtikrinimo veiksmų sekos buvo sėkmingai paleistos ir įvykdytos.

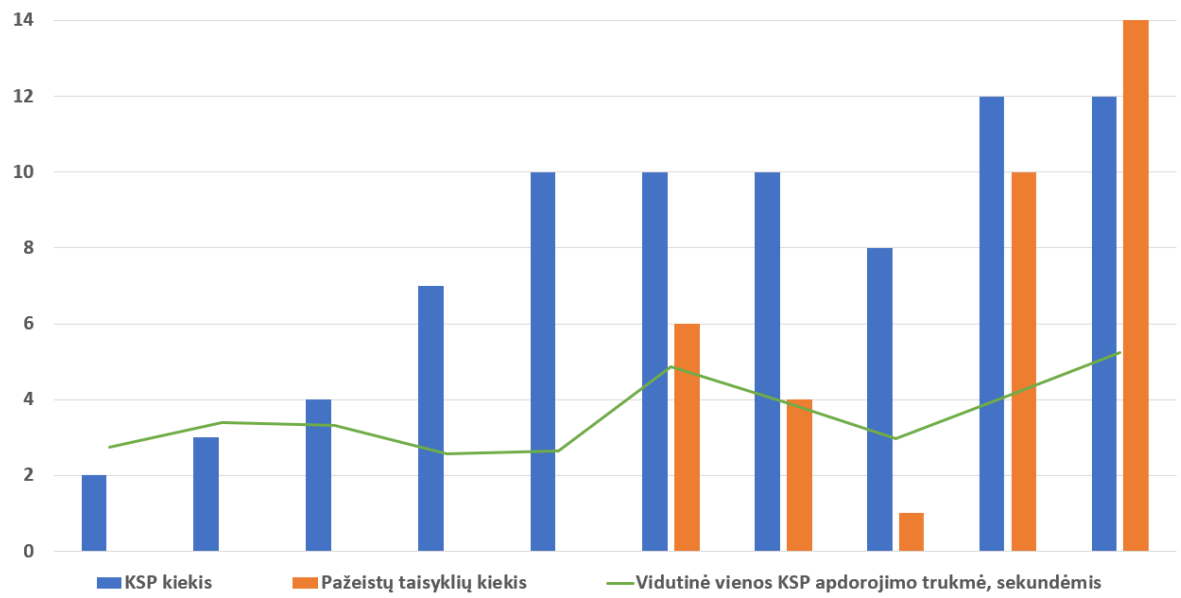
4.5. IT saugos politikos automatizuoto valdymo sistemos kiekybinis tyrimas

Šio tyrimo tikslas – išmatuoti KSP apdorojimo trukmės priklausomybę nuo neatitikčių kiekio. Bandymo metu buvo tyčia inicijuotos skirtingų tipų neatitiktys. Viso atlikta 10 bandymų, kiekvieno bandymo metu pažeistų kompiuterizuotų saugumo politikų taisyklių kiekiai buvo didinami pradedant nuo nulio. Kiekvienas bandymas buvo kartojamas po tris kartus ir lentelėje buvo registruojama didžiausia vykdymo laiko reikšmė. Vykdymo laikas prieš jį registruojant lentelėje buvo suapvalinamas paliekant du skaičius po kablelio. 4.8 lentelėje pateikti kiekybinio tyrimo rezultatai.

4.8 lentelė. Kiekybinio tyrimo rezultatai

Bandymo numeris	Vykdymo trukmė, sekundėmis	KSP kiekis	Pažeistų taisyklių kiekis	Vidutinė vienos KSP apdorojimo trukmė, sekundėmis
1	5,47	2	0	2.73
2	10,17	3	0	3.39
3	13,28	4	0	3.32
4	17,98	7	0	2.56
5	26,56	10	0	2.65
6	48,73	10	6	4.87
7	39,32	10	4	3.93
8	23,85	8	1	2.98
9	49,12	12	10	4.09
10	62.79	12	14	5.23

4.8 pav. yra grafiškai pavaizduoti kiekybinio tyrimo rezultatai.



4.8 pav. Kiekybinio tyrimo rezultatų diagrama

Iš lentelėje pateiktų rezultatų iškart galima padaryti išvadą, kad vidutinė vienos KSP apdorojimo trukmė tiesiogiai nepriklauso nuo KSP kiekio, tačiau tiesiogiai priklauso nuo pažeistų taisyklių kiekio. Vidutinė vienos KSP apdorojimo trukmė svyruoja tarp 2.56 ir 5.23 sekundės. Spėjama, kad svyravimas gaunasi toks didelis todėl, kad bandymo metu buvo inicijuojamos ne vieno, o įvairių tipų neatitiktys. Manoma, kad atliekant šį tyrimą su vieno tipo neatitiktimis, šis svyravimas būtų gerokai mažesnis. Tyrimo vykdymo metu buvo pastebėta, kad *MWDTrafficRule* tipo taisyklės turi tendenciją būti apdorojamos ilgiau, kadangi iš tikrųjų šio tipo taisyklių atitikties tikrinimo ir užtikrinimo komandų generavimas ir vykdymas užtrunka ilgiau negu kad, pavyzdžiui, *ADMXRule*. Taip pat aptikus *MWDTrafficRule_Incompliance* tipo neatitiktį neretai tenka paleisti keletą PowerShell komandų reikalingų neteisingai sukonfigūruoto parametro išsiaiškinimui (tam, kad klaidingai sukonfigūruotą parametrą būtų galima atvaizduoti ataskaitoje). Taigi, tyrimo metu pasitvirtino faktas, kad didėjant pažeistų taisyklių kiekiui ilgėja ir politikos apdorojimo laikas. Tai patvirtina žalios linijos tendencija kilti į viršų didėjant pažeistų taisyklių skaičiui ir leistis į apačią jam mažėjant.

4.6. Išvados

Atlikus prototipo tyrimą galima padaryti išvadas:

1. Sistemos prototipas sėkmingai apdoroja visas KSP aprašytas taisykles (*ADMXRule, MWDProfileRule, MWDTrafficRule*).
2. Sistemos prototipas sugeba aptikti klaidingas registrų reikšmes ir jas perkonfigūruoti pagal KSP taisykles.
3. Sistemos prototipas sugeba aptikti klaidingą tinklo profilių konfigūraciją ir ją pakeisti pagal KSP taisykles.
4. Sistemos prototipas sugeba aptikti klaidingai sukonfigūruotas ugniasienės taisykles ir jas perkonfigūruoti pagal KSP taisykles.
5. Sistemos prototipas sugeba aptikti KSP neaprašytas taisykles ir jas pašalinti.
6. Sistemos prototipas sugeba aptikti ir ištaisyti su GP objektais susijusias neatitiktis (neįgalinimas, neegzistavimas, priskyrimas neteisingam OV). Tai rodo sistemos perspektyvą dirbti su grupės politikų automatizaivimu ir plėtoti sistemą toliau, kad ji galėtų veikti su kitų tipų GP taisyklėmis, kurios realizuojamos KSP.

5. IT SAUGOS POLITIKOS AUTOMATIZUOTO VALDYMO SISTEMOS ANALIZĖS, PROJEKTAVIMO IR REALIZAVIMO IŠVADOS

Šiame projekte pristatyta saugos politika, su ja susiję iššūkiai bei egzistuojantys IT saugos politikos automatizuoto valdymo įrankiai ir modeliai. Projektinėje dalyje buvo pasiūlyta kompiuterizuotos žemo lygio saugumo politikos XML formatu struktūra ir universalus IT saugos politikos automatizuoto valdymo prototipas, paremtas atitikties tikrinimo ir užtikrinimo programinių veiksmų sekų generavimu ir vykdymu. Realizacijos dalyje remiantis projektinėje dalyje aprašytu modeliu buvo sukurtas sistemos prototipas automatizuojantis Active Directory grupės politikų konfigūravimą ir atitikties valdymą. Prototipo tyrimo metu paaiškėjo, kad įgyvendintas prototipas veikia sklandžiai bei geba aptikti ir pašalinti tyčia inicijuotas neatitiktis.

Pabaigai galima padaryti šias išvadas:

1. Saugos politika turi gyvavimo ciklą, todėl periodiškai turi būti peržiūrima ir atnaujinama.
2. Palaikyti aukštą saugos politikos atitikties organizacijoje lygį gali būti didelis iššūkis, kadangi neretai yra sudėtinga suvaldyti žmogiškojo bei organizacinio faktorių ir šešėlinės saugos keliamą grėsmę.
3. IT saugos politikos automatizuoto valdymo modelis yra potencialus sprendimas organizacijoms, siekiančioms apsaugoti savo infrastruktūrą nuo netinkamai sukonfigūruotų įrenginių.
4. Žemo lygio saugumo politikos konvertavimas į kompiuterizuotą saugumo politiką yra svarbus žingsnis prieš pradedant naudoti IT saugos politikos automatizuoto valdymo sistemą.
5. Tekstinės žemo lygio saugumo politikos kompiuterizavimas yra rankiniu būdu atliekama užduotis. Siekiant patobulinti modelį ir sutaupyti daugiau žmogiškųjų resursų rekomenduojama sukurti metodą (galbūt pasitelkiant dirbtinio intelekto technologiją), atliekantį tekstinės žemo lygio saugumo politikos kompiuterizavimą automatiškai.
6. Automatizuotas saugos politikos atitikties valdymas padeda sutaupyti laiko ir išvengti žmogiškųjų klaidų atsiradimo.

LITERATŪROS SĄRAŠAS

1. Alotaibi, Mutlaq, Steven Furnell, and Nathan Clarke. „*Information security policies: A review of challenges and influencing factors.*“ 2016 11th International Conference for Internet Technology and Secured Transactions (2016).
2. Bowden Joel, S. „*Security Policy: What it is and Why - The Basics*“ (2001).
3. Force, Joint Task, and Transformation Initiative. „*Security and privacy controls for federal information systems and organizations.*“ NIST Special Publication 800.53 (2013).
4. Jastiuginas, Saulius. "*Integralus informacijos saugumo valdymo modelis.*" Informacijos mokslai 61 (2012).
5. Baskerville, Richard, Paolo Spagnoletti, and Jongwoo Kim. „*Incident-centered information security: Managing a strategic balance between prevention and response*.“ Information & management 51.1 (2014): 138-151.
6. International Organization for Standardization. ISO/IEC 27005:2018.
7. International Organization for Standardization. ISO/IEC 27036-1:2021.
8. International Organization for Standardization. ISO/IEC 27014:2020.
9. International Organization for Standardization. ISO/IEC 27001:2022.
10. Kaušpadienė, L., Čenys, A., Goranin, N., Tjoa, S., & Ramanauskaitė, S. „*High-level self-sustaining information security management framework*“ (2017).
11. Maasberg, Michele, John Warren, and Nicole L. Beebe. „*The dark side of the insider: detecting the insider threat through examination of dark triad personality traits.*“ 2015 48th Hawaii International Conference on System Sciences. IEEE, 2015.
12. Eurostat statistics. „*ICT security in enterprises*“, EU-27, 2019 (% enterprises), https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:ICT_security_in_enterprises,_EU-27,_2019_(%25_enterprises).png, paskutinį kartą tikrinta 2023/03/02.
13. Appel, Xinming OV Sudhakar Govindavajhala Andrew. "*Network Security Management with High-level Security Policies*".
14. Dimitrov Vladimir, Kaloyanova Kalinka, Petrov, Milen. „*Adapted SANS Cybersecurity Policies for NIST Cybersecurity Framework“* (2021).
15. SANS Security Policy Templates, https://www.sa.ns.org/information-security-policy/, paskutinį kartą tikrinta 2023/03/13.

16. Security Policy Management Automation Across the Entire Cisco Environment, https://www.algosec.com/wp-content/uploads/2017/01/170108_algosec_cisco_solution_brief.pdf, paskutinį kartą tikrinta 2023/03/13.
17. AlgoSec Firewall Analyzer, https://www.algosec.com/docs/en/asms/a30.00/PDFs/FirewallAnalyzer-UserGuide.pdf, paskutinį kartą tikrinta 2023/03/13.
18. AlgoSec FireFlow, https://www.algosec.com/docs/en/asms/a30.00/PDFs/FireFlow-ConfigurationGuide.pdf, paskutinį kartą tikrinta 2023/03/13.
19. AlgoSec CloudFlow, https://www.algosec.com/wp-content/uploads/pdf/CloudFlow-DS.pdf, paskutinį kartą tikrinta 2023/03/13.
20. Tufin Orchestration Suite, https://lp.tufin.com/rs/769-ICF-145/images/tufin-orchestration-suite-brochure.pdf, paskutinį kartą tikrinta 2023/03/13.
21. XACML Architecture, https://docs.wso2.com/display/IS530/XACML+Architecture, paskutinį kartą tikrinta 2023/03/14.
22. Define, update, share, and enforce policies using code.https://developer.ibm.com/articles/policy-as-code-ansible-automation-engine-and-open-policy-agent/, paskutinį kartą tikrinta 2023/03/14.
23. Ali, Aamir. „*Implementation of New Security Features in CMSWEB Kubernetes Cluster at CERN*“. No. CERN-STUDENTS-Note-2022-138. 2022.
24. Ramosaj, Berim, Berisha, Gentrit. "Systems theory and systems approach to leadership." ILIRIA international review 4.1 (2014): 59-76.

PRIEDAI

1 Priedas. Grupės politikos egzistavimo tikrinimo ir užtikrinimo PowerShell funkcijos

```
function EnforceGPOExistence() {
    Param ([string]$GroupPolicyName)

    if ($ConfigurationFromScratchMode) {
        RunGPOCreationCommand -GroupPolicyName $GroupPolicyName | Out-Null
    } else {
        $ListOfAllGPO = $(Get-GPO -all -Domain $Domain.dnsroot).ForEach({ $_.DisplayName })

        if ($ListOfAllGPO -notcontains $GroupPolicyName) {
            $IncomplianceDescription = "GP pavadinimu '$($GroupPolicyName)' neegzistuoja."
            Write-Output "Aptikta neatitiktis! $($IncomplianceDescription)" | Red
            $SuccessfullyEnforced = RunGPOCreationCommand -GroupPolicyName $GroupPolicyName

            $Missing_GPO = [PSCustomObject]@{
                'Neatitikties ID'                = $Missing_GPO_Incompliance_List.Count + 1
                'Neatitikties tipas'             = "Missing_GPO"
                'Domenas'                        = $Domain.dnsroot
                'KSP ID'                         = $CurrentPolicyObject.Policy.PolicyID
                'GP pavadinimas'                 = $CurrentPolicyObject.Policy.GroupPolicyName
                'Neatitikties aprašymas'         = $IncomplianceDescription
                'Aptikimo laikas'                = Get-Date
                'Atitiktis sėkmingai užtikrinta' = $SuccessfullyEnforced
            }
            $Missing_GPO_Incompliance_List.Add($Missing_GPO)
        }
    }
}

function RunGPOCreationCommand() {
    Param ([string]$GroupPolicyName)
    $SuccessfullyEnforced = $true

    try {
        Invoke-Expression "New-GPO -Name '$($GroupPolicyName)' -Comment '$($GroupPolicyName)' | Out-
        Null"
    }
    catch {
        $SuccessfullyEnforced = $false
    }
    finally {
        if ($SuccessfullyEnforced) {
            Write-Output "GP pavadinimu '$($GroupPolicyName)' sukurta sėkmingai." | Green
        }
        else {
            Write-Output "GP pavadinimu '$($GroupPolicyName)' sukūrimas nepavyko." | Red
        }
    }

    return $SuccessfullyEnforced
}
```

2 Priedas. Grupės politikos įgalinimo tikrinimo ir užtikrinimo PowerShell funkcijos

```
function EnforceGPOEnablement() {
    Param ([string]$GroupPolicyName)

    $GPOObject = Get-GPO -Name $GroupPolicyName.Substring($GroupPolicyName.IndexOf("\") + 1)

    if ($ConfigurationFromScratchMode) {
        RunGPOEnablementCommand -GPOObject $GPOObject | Out-Null
    }
    else {
        if ($GPOObject.GpoStatus -ne "AllSettingsEnabled") {
            $IncomplianceDescription = "GP pavadinimu '$($GroupPolicyName)' statusas nėra
            'AllSettingsEnabled'."
            Write-Output "Aptikta neatitiktis! $($IncomplianceDescription)." | Red
            $SuccessfullyEnforced = RunGPOEnablementCommand -GPOObject $GPOObject
            $Disabled_GPO = [PSCustomObject]@{
                'Neatitikties ID'                = $Disabled_GPO_Incompliance_List.Count + 1
                'Neatitikties tipas'             = "Disabled_GPO"
                'Domenas'                        = $Domain.dnsroot
                'KSP ID'                         = $CurrentPolicyObject.Policy.PolicyID
                'GP pavadinimas'                 = $CurrentPolicyObject.Policy.GroupPolicyName
                'Neatitikties aprašymas'         = $IncomplianceDescription
                'Aptikimo laikas'                = Get-Date
                'Atitiktis sėkmingai užtikrinta' = $SuccessfullyEnforced
            }
            $Disabled_GPO_Incompliance_List.Add($Disabled_GPO)
            Write-Output "GP pavadinimu '$($CurrentPolicyObject.Policy.GroupPolicyName)' statusas
            sėkmingai pakeistas į 'AllSettingsEnabled'." | Green
        }
    }
}

function RunGPOEnablementCommand() {
    Param ([object]$GPOObject)
    $SuccessfullyEnforced = $true
    try {
        $GPOObject.GpoStatus = "AllSettingsEnabled"
    }
    catch {
        $SuccessfullyEnforced = $false
    }
    finally {
        if ($SuccessfullyEnforced) {
            Write-Output "GP pavadinimu '$($GroupPolicyName)' sėkmingai įgalinta." | Green
        }
        else {
            Write-Output "GP pavadinimu '$($GroupPolicyName)' įgalinimas nepavyko." | Red
        }
    }
    return $SuccessfullyEnforced
}
```

3 Priedas. Grupės politikos taikymo organizaciniam vienetui tikrinimo ir užtikrinimo PowerShell funkcijos

```
function EnforceGPOapplicationToOU() {
    Param ([string]$GroupPolicyName)

    $CurrentlyAppliedOUlist = GetDistinguishedNamesOfGPO -GroupPolicyName
$CurrentPolicyObject.Policy.GroupPolicyName

    foreach ($DistinguishedName in GetApplyToObjects) {
        if ($ConfigurationFromScratchMode) {
            RunGPOapplicationToOUcommand -GroupPolicyName $GroupPolicyName -DistinguishedName
$DistinguishedName | Out-Null
        }
        else {
            if ($CurrentlyAppliedOUlist -contains $DistinguishedName) {
                continue
            }
            else {
                $IncomplianceDescription = "GP pavadinimu
                '$($CurrentPolicyObject.Policy.GroupPolicyName)' netaikoma '$($DistinguishedName)'."
                Write-Output "Aptikta neatitiktis! $($IncomplianceDescription)" | Red
                $SuccessfullyEnforced = RunGPOapplicationToOUcommand -GroupPolicyName
                $GroupPolicyName -DistinguishedName $DistinguishedName
                $GPO_appliance_to_OU_Incompliance = [PSCustomObject]@{
                    'Neatitikties ID'             = $GPO_appliance_to_OU_Incompliance_List.Count + 1
                    'Neatitikties tipas'          = "GPO_appliance_to_OU_Incompliance"
                    'Domenas'                     = $Domain.dnsroot
                    'KSP ID'                      = $CurrentPolicyObject.Policy.PolicyID
                    'GP pavadinimas'              = $CurrentPolicyObject.Policy.GroupPolicyName
                    'OV'                             = $DistinguishedName
                    'Neatitikties aprašymas'         = $IncomplianceDescription
                    'Aptikimo laikas'                = Get-Date
                    'Atitiktis sėkmingai užtikrinta' = $SuccessfullyEnforced
                }
                $GPO_appliance_to_OU_Incompliance_List.Add($GPO_appliance_to_OU_Incompliance)
            }
        }
    }
}

function RunGPOapplicationToOUcommand {
    Param ([string]$GroupPolicyName, [string]$DistinguishedName)
    $SuccessfullyEnforced = $true
    try {
        Invoke-Expression "New-GPLink -Name '$($GroupPolicyName)' -Target '$($DistinguishedName)' |
Out-Null"
    }
    catch {
        $SuccessfullyEnforced = $false
    }
    finally {
        if ($SuccessfullyEnforced) {
            Write-Output "GP pavadinimu '$($GroupPolicyName)' sėkmingai pritaikyta
'$($DistinguishedName)'." | Green
        }
        else {
            Write-Output "GP pavadinimu '$($GroupPolicyName)' pritaikymas '$($DistinguishedName)'
nepavyko." | Red
        }
    }
    return $SuccessfullyEnforced
}
```

4 Priedas. Grupės politikos taikymo klaidingam organizaciniam vienetui aptikimo ir ištaisymo PowerShell funkcijos

```
function EnforceGPOnonapplicationToWrongOU() {
    Param ([string]$GroupPolicyName)

    $ShouldBeAppliedOUlist = GetApplyToObjects

    $CurrentlyAppliedOUlist = GetDistinguishedNamesOfGPO -GroupPolicyName
$CurrentPolicyObject.Policy.GroupPolicyName

    foreach ($CurrentDistinguishedName in $CurrentlyAppliedOUlist) {
        if ($ConfigurationFromScratchMode) {
            continue
        }
        else {
            if ($ShouldBeAppliedOUlist -notcontains $CurrentDistinguishedName) {
                $IncomplianceDescription = "GP pavadinimu
                '$($CurrentPolicyObject.Policy.GroupPolicyName)' neturi būti taikoma
                '$($CurrentDistinguishedName)'."
                Write-Output "Aptikta neatitiktis! $($IncomplianceDescription)" | Red
                $SuccessfullyEnforced = RunGPOunlinkingfromOUcommand -GroupPolicyName
                $GroupPolicyName -DistinguishedName $CurrentDistinguishedName
                $GPO_appliance_to_OU_Incompliance = [PSCustomObject]@{
                 'Neatitikties ID'                = $GPO_appliance_to_OU_Incompliance_List.Count + 1
                 'Neatitikties tipas'             = "GPO_appliance_to_OU_Incompliance"
                 'Domenas'                        = $Domain.dnsroot
                 'KSP ID'                         = $CurrentPolicyObject.Policy.PolicyID
                 'GP pavadinimas'                 = $CurrentPolicyObject.Policy.GroupPolicyName
                 'OV'                             = $CurrentDistinguishedName
                 'Neatitikties aprašymas'         = $IncomplianceDescription
                 'Aptikimo laikas'                = Get-Date
                 'Atitiktis sėkmingai užtikrinta' = $SuccessfullyEnforced
                }
                $GPO_appliance_to_OU_Incompliance_List.Add($GPO_appliance_to_OU_Incompliance)
            }
        }
    }
}

function RunGPOunlinkingfromOUcommand {
    Param ([string]$GroupPolicyName, [string]$DistinguishedName)

    $SuccessfullyEnforced = $true

    try {
        Invoke-Expression "Remove-GPLink -Name '$($GroupPolicyName)' -Target '$($DistinguishedName)'
| Out-Null"
    }
    catch {
        $SuccessfullyEnforced = $false
    }
    finally {
        if ($SuccessfullyEnforced) {
            Write-Output "GP pavadinimu '$($GroupPolicyName)' taikymas sėkmingai nutrauktas
'$($DistinguishedName)'." | Green
        }
        else {
            Write-Output "GP pavadinimu '$($GroupPolicyName)' taikymo '$($DistinguishedName)'
nutraukimas nepavyko." | Red
        }
    }

    return $SuccessfullyEnforced
}
```

5 Priedas. *ADMXRule* taisyklės atitikties tikrinimo ir užtikrinimo PowerShell funkcijos

```
function EnforceADMXPolicyCompliance() {
    $RuleNumber = 0
    $Rules = GetRulesList($CurrentPolicyObject)

    foreach ($Rule in $Rules) {
        $RuleNumber = $RuleNumber + 1

        if ($ConfigurationFromScratchMode) {
            RunADMXRuleEnforcementCommand -Rule $Rule -RuleNumber $RuleNumber | Out-Null
        }
        else {
            Write-Output "Tikrinama kompiuterizuotos saugumo politikos taisyklės numeriu
            '$($RuleNumber)' atitiktis.." | Yellow

            $validationCommandOutput = Invoke-Expression
            "$($CurrentPolicyObject.Policy.ValidationFunction) -Name '$($Rule.Name)' -Key
            '$($Rule.Key)' -ValueName '$($Rule.ValueName)' -ErrorAction SilentlyContinue"

            if (!($validationCommandOutput.Value -eq $Rule.Value)) {
                $IncomplianceDescription = "Neteisinga registro '$($Rule.Key)\$($Rule.ValueName)'
                reikšmė"
                Write-Output "Aptikta kompiuterizuotos saugumo politikos taisyklės neatitiktis!
                $($IncomplianceDescription)" | Red

                $SuccessfullyEnforced = RunADMXRuleEnforcementCommand -Rule $Rule -RuleNumber
                $RuleNumber

                $ADMXRule_Incompliance = [PSCustomObject]@{
                'Neatitikties ID'                       = $ADMXRule_Incompliance_List.Count + 1
                'Neatitikties tipas'                    = "ADMXRule_Incompliance"
                'Domenas'                               = $Domain.dnsroot
                'KSP ID'                                = $CurrentPolicyObject.Policy.PolicyID
                'GP pavadinimas'                        = $CurrentPolicyObject.Policy.GroupPolicyName
                'Neatitikties aprašymas'                = $IncomplianceDescription
                'Tekstinės saugumo politikos aprašymas' = $CurrentPolicyObject.Policy.Description
                'Taisyklės eilės numeris'               = $RuleNumber
                'Aptikimo laikas'                       = Get-Date
                'Atitiktis sėkmingai užtikrinta'        = $SuccessfullyEnforced
                }

                $ADMXRule_Incompliance_List.Add($ADMXRule_Incompliance)
            }
        }
    }

    Write-Output "Kompiuterizuotos saugumo politikos (ID -
'$($CurrentPolicyObject.Policy.PolicyID)') atitiktis sėkmingai užtikrinta." | Green
}

function RunADMXRuleEnforcementCommand {
    Param ([object]$Rule, [int]$RuleNumber)

    $SuccessfullyEnforced = $true

    try {
        Invoke-Expression "$($CurrentPolicyObject.Policy.EnforcementFunction) -Name '$($Rule.Name)'
        -Key '$($Rule.Key)' -ValueName '$($Rule.ValueName)' -Type '$($Rule.Type)' -Value
        $($Rule.Value)" | Out-Null
    }
    catch {
        $SuccessfullyEnforced = $false
    }
    finally {
        if ($SuccessfullyEnforced) {
            Write-Output "Kompiuterizuotos saugumo politkos taisyklės numeriu '$($RuleNumber)'
            atitiktis užtikrinta sėkmingai." | Green
        }
        else {
            Write-Output "Kompiuterizuotos saugumo politkos taisyklės numeriu '$($RuleNumber)'
            atitikties užtikrinimas nepavyko." | Red
        }
    }
    return $SuccessfullyEnforced
}
```

6 Priedas. *MWDProfileRule* taisyklės atitikties tikrinimo ir užtikrinimo PowerShell funkcijos

```
function EnforceMWDProfilePolicyCompliance() {
    $RuleNumber = 0
    $Rules = GetRulesList($CurrentPolicyObject)

    foreach ($Rule in $Rules) {
        $RuleNumber = $RuleNumber + 1

        if ($ConfigurationFromScratchMode) {
            RunMWDProfileRuleEnforcementCommand -Rule $Rule -RuleNumber $RuleNumber | Out-Null
        }
        else {
            Write-Output "Tikrinama kompiuterizuotos saugumo politikos taisyklės numeriu
            '$($RuleNumber)' atitiktis.." | Yellow

            $checkCommand = "$($CurrentPolicyObject.Policy.ValidationFunction) -Name '$($Rule.Name)'
            -PolicyStore '$($Rule.PolicyStore)'" -replace '\s+', ' '

            $ValuesAndTheirEqualityWithRuleValuesTupple = New-Object
            'Collections.Generic.List[Tuple[bool,string,string]]'

            $ValidationCommandOutput = Invoke-Expression $checkCommand
            $RulePropertiesCount = $(($Rule | Get-Member -MemberType Property).count) - 1
            $RuleProperties = $Rule.PSObject.Properties | Select-Object -Expand Name

            foreach ($RuleProperty in $RuleProperties[0 .. $RulePropertiesCount]) {
             $OutputValue = ($ValidationCommandOutput | Select-Object -ExpandProperty $RuleProperty)
             $RuleValue = ($Rule | Select-Object -ExpandProperty $RuleProperty)
             $ProfileValue = ($Rule | Select-Object -ExpandProperty "Name")
             $EqualOrNot = ($OutputValue -eq $RuleValue)

             $ValuesAndTheirEqualityWithRuleValuesTupple.Add([Tuple]::Create($EqualOrNot,
             $RuleProperty, $ProfileValue))
            }

            $ValuesAndTheirEqualityWithRuleValuesTupple | ForEach-Object {
                if (!($_.Item1) -and $_.Item2 -ne "PolicyStore") {
                    $IncomplianceDescription = "Neteisinga parametro '$($_.Item2)' reikšmė
                    '$($_.Item3)' profilyje"

                    Write-Output "Aptikta kompiuterizuotos saugumo politikos taisyklės neatitiktis!
                    $($IncomplianceDescription)" | Red

                    $SuccessfullyEnforced = RunMWDProfileRuleEnforcementCommand -Rule $Rule -
                    RuleNumber $RuleNumber

                    $MWDProfileRule_Incompliance = [PSCustomObject]@{
                    'Neatitikties ID'              = $MWDProfileRule_Incompliance_List.Count + 1
                    'Neatitikties tipas'                    = "MWDProfileRule_Incompliance"
                    'Domenas'                               = $Domain.dnsroot
                    'KSP ID'                                = $CurrentPolicyObject.Policy.PolicyID
                    'GP pavadinimas'               = $CurrentPolicyObject.Policy.GroupPolicyName
                    'Neatitikties aprašymas'                = $IncomplianceDescription
                    'Tekstinės saugumo politikos aprašymas' = $CurrentPolicyObject.Policy.Description
                    'Taisyklės eilės numeris'               = $RuleNumber
                    'Aptikimo laikas'                       = Get-Date
                    'Atitiktis sėkmingai užtikrinta'        = $SuccessfullyEnforced
                    }

                    $MWDProfileRule_Incompliance_List.Add($MWDProfileRule_Incompliance)
                    Continue
                }
            }
        }
    }

    Write-Output "Kompiuterizuotos saugumo politikos (ID -
'$($CurrentPolicyObject.Policy.PolicyID)') atitiktis sėkmingai užtikrinta." | Green
}
```

```powershell
function RunMWDProfileRuleEnforcementCommand {
    Param ([object]$Rule, [int]$RuleNumber)

    $SuccessfullyEnforced = $true

    $EnforcementCommand = "$($CurrentPolicyObject.Policy.EnforcementFunction)
    $(if ($Rule.Name){" -Name '$($Rule.Name)'"})
    $(if ($Rule.PolicyStore){" -PolicyStore '$($Rule.PolicyStore)'"})
    $(if ($Rule.Enabled){" -Enabled $($Rule.Enabled)"})
    $(if ($null -ne $Rule.DefaultInboundAction){" -DefaultInboundAction
    '$($Rule.DefaultInboundAction)'"} if ($null -ne $Rule.DefaultOutboundAction) {"
    -DefaultOutboundAction '$($Rule.DefaultOutboundAction)'"})
    $(if ($Rule.AllowInboundRules){" -AllowInboundRules $($Rule.AllowInboundRules)"})
    $(if ($Rule.AllowLocalFirewallRules){" -AllowLocalFirewallRules
    $($Rule.AllowLocalFirewallRules)"})
    $(if ($Rule.AllowLocalIPsecRules){" -AllowLocalIPsecRules $($Rule.AllowLocalIPsecRules)"})
    $(if ($Rule.AllowUserApps){" -AllowUserApps $($Rule.AllowUserApps)"})
    $(if ($Rule.AllowUserPorts){" -AllowUserPorts $($Rule.AllowUserPorts)"})
    $(if ($Rule.AllowUnicastResponseToMulticast){" -AllowUnicastResponseToMulticast
    $($Rule.AllowUnicastResponseToMulticast)"})
    $(if ($Rule.NotifyOnListen){" -NotifyOnListen $($Rule.NotifyOnListen)"})
    $(if ($Rule.EnableStealthModeForIPsec){" -EnableStealthModeForIPsec
    $($Rule.EnableStealthModeForIPsec)"})
    $(if ($Rule.LogFileName){" -LogFileName $($Rule.LogFileName)"})
    $(if ($Rule.LogMaxSizeKilobytes){" -LogMaxSizeKilobytes $($Rule.LogMaxSizeKilobytes)"})
    $(if ($Rule.LogAllowed){" -LogAllowed $($Rule.LogAllowed)"})
    $(if ($Rule.LogBlocked){" -LogBlocked $($Rule.LogBlocked)"})
    $(if ($Rule.LogIgnored){" -LogIgnored $($Rule.LogIgnored)"})
    $(if ($Rule.DisabledInterfaceAliases){" -DisabledInterfaceAliases
    $($Rule.DisabledInterfaceAliases)"})" -replace '\s+', ' '

    try {
        Invoke-Expression $EnforcementCommand
    }
    catch {
        $SuccessfullyEnforced = $false
    }
    finally {
        if ($SuccessfullyEnforced) {
            Write-Output "Kompiuterizuotos saugumo politkos taisyklės numeriu '$($RuleNumber)'
            atitiktis užtikrinta sėkmingai." | Green
        }
        else {
            Write-Output "Kompiuterizuotos saugumo politkos taisyklės numeriu '$($RuleNumber)'
            atitikties užtikrinimas nepavyko." | Red
        }
    }
    return $SuccessfullyEnforced
}
```

7 Priedas. *MWDTrafficRule* taisyklės atitikties tikrinimo ir užtikrinimo PowerShell funkcijos

```
function EnforceMWDTrafficPolicyCompliance() {
    $RuleNumber = 0
    $Rules = GetRulesList($CurrentPolicyObject)

    foreach ($Rule in $Rules) {

        $RuleNumber = $RuleNumber + 1

        if ($ConfigurationFromScratchMode) {

            RunMWDTrafficRuleEnforcementCommand -Rule $Rule -RuleNumber $RuleNumber | Out-Null

        }
        else {

            Write-Output "Tikrinama kompiuterizuotos saugumo politikos taisyklės numeriu
            '$($RuleNumber)' atitiktis.." | Yellow

            $ValidationCommand = "$($CurrentPolicyObject.Policy.ValidationFunction)
            $(if ($Rule.PolicyStore){" -PolicyStore '$($Rule.PolicyStore)'"})
            $(if (!$Rule.Name){"| Where-Object Name -eq '$($Rule.Name)'"})
            $(if ($Rule.DisplayName){"| Where-Object DisplayName -eq '$($Rule.DisplayName)'"})
            $(if ($Rule.Description){"| Where-Object Description -eq '$($Rule.Description)'"})
            $(if ($Rule.DisplayGroup){"| Where-Object DisplayGroup -eq '$($Rule.DisplayGroup)'"})
            $(if ($Rule.Group){"| Where-Object Group -eq '$($Rule.Group)'"})
            $(if ($Rule.Enabled){"| Where-Object Enabled -eq '$($Rule.Enabled)'"})
            $(if ($Rule.Profile){"| Where-Object Profile -eq '$($Rule.Profile)'"})
            $(if ($Rule.Platform){"| Where-Object Platform -eq '$($Rule.Platform)'"})
            $(if ($Rule.Direction){"| Where-Object Direction -eq '$($Rule.Direction)'"})
            $(if ($Rule.Action){"| Where-Object Action -eq '$($Rule.Action)'"})
            $(if ($Rule.EdgeTraversalPolicy){"| Where-Object EdgeTraversalPolicy -eq
            '$($Rule.EdgeTraversalPolicy)'"})
            $(if ($Rule.LooseSourceMapping){"| Where-Object LooseSourceMapping -eq
            '$($Rule.LooseSourceMapping)'"})
            $(if ($Rule.LocalOnlyMapping){"| Where-Object LocalOnlyMapping -eq
            '$($Rule.LocalOnlyMapping)'"})
            $(if ($Rule.Owner){"| Where-Object Owner -eq '$($Rule.Owner)'"})
            $(if ($Rule.PrimaryStatus){"| Where-Object PrimaryStatus -eq '$($Rule.PrimaryStatus)'"})
            $(if ($Rule.Status){"| Where-Object Status -eq '$($Rule.Status)'"})
            $(if ($Rule.EnforcementStatus){"| Where-Object EnforcementStatus -eq
            '$($Rule.EnforcementStatus)'"})
            $(if ($Rule.PolicyStoreSource){"| Where-Object PolicyStoreSource -eq
            '$($Rule.PolicyStoreSource)'"})
            $(if ($Rule.PolicyStoreSourceType){"| Where-Object PolicyStoreSourceType -eq
            '$($Rule.PolicyStoreSourceType)'"})
            | Get-NetFirewallAddressFilter
            $(if ($Rule.LocalAddress){"| Where-Object LocalAddress -eq '$($Rule.LocalAddress)'
            | Where-Object { " + "$" + "_." + "LocalAddress.Count -eq 1 }"})
            $(if ($Rule.LocalAddresses){GenerateWhereObjectContainCommandPartAddresses -objName
            "LocalAddress" -items $Rule.LocalAddresses.LocalAddress})
            $(if ($Rule.RemoteAddress){"| Where-Object RemoteAddress -eq '$($Rule.RemoteAddress)'
            | Where-Object { " + "$" + "_." + "RemoteAddress.Count -eq 1 }"})
            $(if ($Rule.RemoteAddresses){GenerateWhereObjectContainCommandPartAddresses -objName
            "RemoteAddress" -items $Rule.RemoteAddresses.RemoteAddress})
            | Get-NetFirewallRule | Get-NetFirewallPortFilter
            $(if ($Rule.Protocol){"| Where-Object Protocol -eq '$($Rule.Protocol)'"})
            $(if ($Rule.LocalPort){"| Where-Object LocalPort -eq '$($Rule.LocalPort)'
            | Where-Object { " + "$" + "_." + "LocalPort.Count -eq 1 }"})
            $(if ($Rule.LocalPorts){GenerateWhereObjectContainCommandPart -objName "LocalPort" -
            items $Rule.LocalPorts.LocalPort})
            $(if ($Rule.RemotePort){"| Where-Object RemotePort -eq '$($Rule.RemotePort)'
            | Where-Object { " + "$" + "_." + "RemotePort.Count -eq 1 }"})
            $(if ($Rule.RemotePorts){GenerateWhereObjectContainCommandPart -objName "RemotePort" -
            items $Rule.RemotePorts.RemotePort})
            $(if ($Rule.IcmpType){"| Where-Object IcmpType -eq '$($Rule.IcmpType)'
            | Where-Object { " + "$" + "_." + "IcmpType.Count -eq 1 }"})
            $(if ($Rule.IcmpTypes){GenerateWhereObjectContainCommandPart -objName "IcmpType" -items
            $Rule.IcmpTypes.IcmpType})
            $(if ($Rule.DynamicTarget){"| Where-Object DynamicTarget -eq '$($Rule.DynamicTarget)'"})
            | Get-NetFirewallRule | Get-NetFirewallApplicationFilter
            $(if ($Rule.Program){"| Where-Object Program -eq '$($Rule.Program)'"})
            $(if ($Rule.Package){"| Where-Object Package -eq '$($Rule.Package)'"})
            $(if ($Rule.Service){"| Get-NetFirewallRule | Get-NetFirewallServiceFilter
            | Where-Object Service -eq '$($Rule.Service)'"})" -replace '\s+', ' '

            $ValidationCommandOutput = Invoke-Expression $ValidationCommand
```

```
            if (($null -ne $ValidationCommandOutput)) {

                AddMWDTrafficRuleGuidToTupleByValue -guid $Rule.Name
                continue

            }

            else {

        $IncompliantParameter = FindMWDTrafficRuleIncompliantParameter -Command $ValidationCommand

        $IncomplianceDescription = "Neteisinga taisyklės parametro '$($IncompliantParameter)'
        reikšmė."

        Write-Output "Aptikta kompiuterizuotos saugumo politikos taisyklės neatitiktis!
        $($IncomplianceDescription)" | Red

        Remove-NetFirewallRule -PolicyStore $Rule.PolicyStore -DisplayName $Rule.DisplayName

        $SuccessfullyEnforced = RunMWDTrafficRuleEnforcementCommand -Rule $Rule -RuleNumber
        $RuleNumber

              $MWDTrafficRule_Incompliance = [PSCustomObject]@{
                'Neatitikties ID'                  = $MWDTrafficRule_Incompliance_List.Count + 1
                'Neatitikties tipas'                    = "MWDTrafficRule Incompliance"
                'Domenas'                               = $Domain.dnsroot
                'KSP ID'                                = $CurrentPolicyObject.Policy.PolicyID
                'GP pavadinimas'                   = $CurrentPolicyObject.Policy.GroupPolicyName
                'Neatitikties aprašymas'                = $IncomplianceDescription
                'Tekstinės saugumo politikos aprašymas' = $CurrentPolicyObject.Policy.Description
                'Taisyklės eilės numeris'               = $RuleNumber
                'Aptikimo laikas'                       = Get-Date
                'Atitiktis sėkmingai užtikrinta'        = $SuccessfullyEnforced
              }

              $MWDTrafficRule_Incompliance_List.Add($MWDTrafficRule_Incompliance)

            }
        }

    }

    Write-Output "Kompiuterizuotos saugumo politikos (ID -
    '$($CurrentPolicyObject.Policy.PolicyID)') atitiktis sėkmingai užtikrinta." | Green

}

function RunMWDTrafficRuleEnforcementCommand {
    Param ([object]$Rule, [int]$RuleNumber)

    $SuccessfullyEnforced = $true

    $EnforcementCommand = "$($CurrentPolicyObject.Policy.EnforcementFunction)
    $(if ($Rule.PolicyStore){" -PolicyStore '$($Rule.PolicyStore)'"})
    $(if ($Rule.GPOSession){" -GPOSession '$($Rule.GPOSession)'"})
    $(if ($Rule.DisplayName){" -DisplayName '$($Rule.DisplayName)'"})
    $(if ($Rule.Description){" -Description '$($Rule.Description)'"})
    $(if ($Rule.Group){" -Group '$($Rule.Group)'"})
    $(if ($Rule.Enabled){" -Enabled '$($Rule.Enabled)'"})
    $(if ($Rule.Profile){" -Profile '$($Rule.Profile)'"})
    $(if ($Rule.Platform){" -Platform '$($Rule.Platform)'"})
    $(if ($Rule.Direction){" -Direction '$($Rule.Direction)'"})
    $(if ($Rule.Action){" -Action '$($Rule.Action)'"})
    $(if ($Rule.EdgeTraversalPolicy){" -EdgeTraversalPolicy '$($Rule.EdgeTraversalPolicy)'"})
    $(if ($Rule.LooseSourceMapping){" -LooseSourceMapping '$($Rule.LooseSourceMapping)'"})
    $(if ($Rule.LocalOnlyMapping){" -LocalOnlyMapping '$($Rule.LocalOnlyMapping)'"})
    $(if ($Rule.Owner){" -Owner '$($Rule.Owner)'"})
    $(if ($Rule.LocalAddress){" -LocalAddress '$($Rule.LocalAddress)'"})
    $(if ($Rule.LocalAddresses){" -LocalAddress $($Rule.LocalAddresses.LocalAddress -join " ,")"})
    $(if ($Rule.RemoteAddress){" -RemoteAddress '$($Rule.RemoteAddress)'"})
    $(if ($Rule.RemoteAddresses){" -RemoteAddress $($Rule.RemoteAddresses.RemoteAddress -join "
    ,")"})
    $(if ($Rule.Protocol){" -Protocol '$($Rule.Protocol)'"})
    $(if ($Rule.LocalPort){" -LocalPort '$($Rule.LocalPort)'"})
    $(if ($Rule.LocalPorts){" -LocalPort $($Rule.LocalPorts.LocalPort -join " ,")"})
    $(if ($Rule.RemotePort){" -RemotePort '$($Rule.RemotePort)'"})
    $(if ($Rule.RemotePorts){" -RemotePort $($Rule.RemotePorts.RemotePort -join " ,")"})
    $(if ($Rule.IcmpType){" -IcmpType '$($Rule.IcmpType)'"})
    $(if ($Rule.IcmpTypes){" -IcmpType $($Rule.IcmpTypes.IcmpType -join " ,")"})
    $(if ($Rule.DynamicTarget){" -DynamicTarget '$($Rule.DynamicTarget)'"})
```

```
    $(if ($Rule.Program){" -Program '$($Rule.Program)'"})
    $(if ($Rule.Package){" -Package '$($Rule.Package)'"})
    $(if ($Rule.Service){" -Service '$($Rule.Service)'"})
    $(if ($Rule.InterfaceAlias){" -InterfaceAlias '$($Rule.InterfaceAlias)'"})
    $(if ($Rule.InterfaceType){" -InterfaceType '$($Rule.InterfaceType)'"})
    $(if ($Rule.LocalUser){" -LocalUser '$($Rule.LocalUser)'"})
    $(if ($Rule.RemoteUser){" -RemoteUser '$($Rule.RemoteUser)'"})
    $(if ($Rule.RemoteMachine){" -RemoteMachine '$($Rule.RemoteMachine)'"})
    $(if ($Rule.Encryption){" -Encryption '$($Rule.Encryption)'"})
    $(if ($Rule.OverrideBlockRules){" -OverrideBlockRules '$($Rule.OverrideBlockRules)'"})
    $(if ($Rule.RemoteDynamicKeywordAddresses){" -RemoteDynamicKeywordAddresses
    '$($Rule.RemoteDynamicKeywordAddresses.RemoteDynamicKeywordAddress -join " ,")'"})" -replace
    '\s+', ' '

    try {
        $EnforcementCommandOutput = Invoke-Expression $EnforcementCommand
        UpdateMWDTrafficRuleNameInXMLPolicy -CurrentPolicyPath $CurrentPolicyPath -RuleNumber
        $RuleNumber
        -EnforcementCommandOutput $EnforcementCommandOutput
    }
    catch {
        $SuccessfullyEnforced = $false
    }
    finally {
        if ($SuccessfullyEnforced) {
            Write-Output "Kompiuterizuotos saugumo politkos taisyklės numeriu '$($RuleNumber)'
            atitiktis užtikrinta sėkmingai." | Green
        }
        else {
            Write-Output "Kompiuterizuotos saugumo politkos taisyklės numeriu '$($RuleNumber)'
            atitikties užtikrinimas nepavyko." | Red
        }
    }
    return $SuccessfullyEnforced
}
```

8 Priedas. Nereikalingos *MWDTrafficRule* taisyklės aptikimo ir pašalinimo PowerShell funkcijos

```
function EnforceAbsenceOfRedundantMWDTrafficRules() {
    Param([Collections.Generic.List[Tuple[string,
System.Collections.Generic.List[string]]]]$GroupPolicyAndItsMWDTrafficRuleGuidsTuple)

    if ($RunOption -eq 'B') {
        $GroupPolicyAndItsMWDTrafficRuleGuidsTuple | ForEach-Object {


[System.Collections.Generic.List[string]]$ListOfMWDTrafficRuleGuidsOfGroupPolicyBeingChecked =
Invoke-Expression "Get-NetFirewallRule -PolicyStore '$($Domain.dnsroot)\$($_.Item1)' | Select-Object
-ExpandProperty Name"

            $MustExistdMWDTrafficRuleGuidList = ($_.Item2)
            $GroupPolicyName = ($_.Item1)

            $ListOfMWDTrafficRuleGuidsOfGroupPolicyBeingChecked | ForEach-Object {
                $MWDTrafficRuleGuid = $_

                if ($MustExistdMWDTrafficRuleGuidList -notcontains $MWDTrafficRuleGuid) {

                    $RedundantRuleDisplayNameCommandOutput = Invoke-Expression "Get-NetFirewallRule
                -PolicyStore '$($Domain.dnsroot)\$($GroupPolicyName)' -Name '$MWDTrafficRuleGuid'"

                    $RedundantRuleDisplayName = $RedundantRuleDisplayNameCommandOutput.DisplayName

                    $IncomplianceDescription = "Aptikta MWDTrafficRule taisyklė, neapibrėžta
                    kompiuterizuotoje saugumo politikoje."

                    Write-Output "Aptikta neatitiktis! $($IncomplianceDescription) Taisyklės GUID -
                '$MWDTrafficRuleGuid', Taisyklės pavadinimas - '$RedundantRuleDisplayName'" | Red

                    $SuccessfullyEnforced = DeleteMWDTrafficRuleByGuid -GroupPolicyName
                    $GroupPolicyName -MWDTrafficRuleGuid $MWDTrafficRuleGuid

                    $Redundant_MWDTrafficRule = [PSCustomObject]@{
                        'Neatitikties ID' = $Redundant_MWDTrafficRule_Incompliance_List.Count + 1
                        'Neatitikties tipas'             = "Redundant_MWDTrafficRule"
                        'Domenas'                        = $Domain.dnsroot
                        'GP pavadinimas'                 = $GroupPolicyName
                        'Neatitikties aprašymas'         = $IncomplianceDescription
                        'Taisyklės GUID'                 = $MWDTrafficRuleGuid
                        'Taisyklės pavadinimas'          = $RedundantRuleDisplayName
                        'Aptikimo laikas'                = Get-Date
                        'Atitiktis sėkmingai užtikrinta' = $SuccessfullyEnforced
                    }

                    $Redundant_MWDTrafficRule_Incompliance_List.Add($Redundant_MWDTrafficRule)

                }
            }
        }
    }
}
```

9 Priedas. Kompiuterizuotos žemo lygio saugumo politikos

1.

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy>
    <Description>Windows Defender ugniasienė turi būti aktyvuota visų Lietuvos padaliniui
priklausančių kompiuterių domeno, privačiame ir viešajame tinklo profiliuose.</Description>
    <PolicyID>1</PolicyID>
    <RuleType>ADMXRule</RuleType>
    <GroupPolicyName>Windows Defender aktyvavimo politika</GroupPolicyName>
    <ApplyTo>
        <DistinguishedName>OU=Kompiuteriai,OU=Lietuvos
         Padalinys,DC=universitetas,DC=local</DistinguishedName>
    </ApplyTo>
    <Rules>
        <ADMXRule>
            <Name>Windows Defender aktyvavimo politika</Name>
               <Key>HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile</Ke
               y>
            <ValueName>EnableFirewall</ValueName>
            <Type>DWORD</Type>
            <Value>1</Value>
        </ADMXRule>
        <ADMXRule>
            <Name>Windows Defender aktyvavimo politika</Name>
               <Key>HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile</
               Key>
            <ValueName>EnableFirewall</ValueName>
            <Type>DWORD</Type>
            <Value>1</Value>
        </ADMXRule>
    </Rules>
    <ValidationFunction>Get-GPRegistryValue</ValidationFunction>
    <EnforcementFunction>Set-GPRegistryValue</EnforcementFunction>
</Policy>
```

2.

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy>
     <Description>Įeinantis tinklo srautas domeno, privačiame bei viešajame tinklo profiliuose,
     neatitinkantis jokios Windows Defender ugniasienės taisyklės turi būti
     blokuojamas.</Description>
    <PolicyID>2</PolicyID>
    <RuleType>MWDProfileRule</RuleType>
    <GroupPolicyName>Windows Defender aktyvavimo politika</GroupPolicyName>
    <ApplyTo>
        <DistinguishedName>OU=Kompiuteriai,OU=Lietuvos
         Padalinys,DC=universitetas,DC=local</DistinguishedName>
    </ApplyTo>
    <Rules>
        <MWDProfileRule>
            <Name>Domain</Name>
            <PolicyStore>universitetas.local\Windows Defender aktyvavimo
               politika</PolicyStore>
            <DefaultInboundAction>Block</DefaultInboundAction>
            <Enabled>True</Enabled>
        </MWDProfileRule>
        <MWDProfileRule>
            <Name>Private</Name>
            <PolicyStore>universitetas.local\Windows Defender aktyvavimo
               politika</PolicyStore>
            <DefaultInboundAction>Block</DefaultInboundAction>
            <Enabled>True</Enabled>
        </MWDProfileRule>
        <MWDProfileRule>
            <Name>Public</Name>
            <PolicyStore>universitetas.local\Windows Defender aktyvavimo
               politika</PolicyStore>
            <DefaultInboundAction>Block</DefaultInboundAction>
            <Enabled>True</Enabled>
        </MWDProfileRule>
    </Rules>
    <ValidationFunction>Get-NetFirewallProfile</ValidationFunction>
    <EnforcementFunction>Set-NetFirewallProfile</EnforcementFunction>
</Policy>
```

3.

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy>
     <Description>Išeinantis tinklo srautas domeno, privačiame bei viešajame tinklo profiliuose,
     neatitinkantis jokios Windows Defender ugniasienės taisyklės yra leidžiamas.</Description>
    <PolicyID>3</PolicyID>
    <RuleType>MWDProfileRule</RuleType>
    <GroupPolicyName>Windows Defender aktyvavimo politika</GroupPolicyName>
    <ApplyTo>
         <DistinguishedName>OU=Kompiuteriai,OU=Lietuvos
         Padalinys,DC=universitetas,DC=local</DistinguishedName>
    </ApplyTo>
    <Rules>
        <MWDProfileRule>
            <Name>Domain</Name>
               <PolicyStore>universitetas.local\Windows Defender aktyvavimo politika</PolicyStore>
            <DefaultOutboundAction>Allow</DefaultOutboundAction>
            <Enabled>True</Enabled>
        </MWDProfileRule>
        <MWDProfileRule>
            <Name>Private</Name>
               <PolicyStore>universitetas.local\Windows Defender aktyvavimo politika</PolicyStore>
            <DefaultOutboundAction>Allow</DefaultOutboundAction>
            <Enabled>True</Enabled>
        </MWDProfileRule>
        <MWDProfileRule>
            <Name>Public</Name>
               <PolicyStore>universitetas.local\Windows Defender aktyvavimo politika</PolicyStore>
            <DefaultOutboundAction>Allow</DefaultOutboundAction>
            <Enabled>True</Enabled>
        </MWDProfileRule>
    </Rules>
    <ValidationFunction>Get-NetFirewallProfile</ValidationFunction>
    <EnforcementFunction>Set-NetFirewallProfile</EnforcementFunction>
</Policy>
```

4.

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy>
     <Description>Domenui priklausančiuose kompiuteriuose draudžiama diegti programinę įrangą, kuri
     nėra leidžiama grupės politikos taisyklių, taip pat draudžiama manipuliuoti prievadų būsena,
     t.y kurti ugniasienės taisykles leidžiančias ar blokuojančias komunikaciją tam tikrais
     prievadais.</Description>
    <PolicyID>4</PolicyID>
    <RuleType>MWDProfileRule</RuleType>
    <GroupPolicyName>Windows Defender aktyvavimo politika</GroupPolicyName>
    <ApplyTo>
         <DistinguishedName>OU=Kompiuteriai,OU=Lietuvos
         Padalinys,DC=universitetas,DC=local</DistinguishedName>
    </ApplyTo>
    <Rules>
        <MWDProfileRule>
            <Name>Domain</Name>
               <PolicyStore>universitetas.local\Windows Defender aktyvavimo politika</PolicyStore>
            <AllowLocalFirewallRules>False</AllowLocalFirewallRules>
            <AllowUserApps>False</AllowUserApps>
            <AllowUserPorts>False</AllowUserPorts>
            <Enabled>True</Enabled>
        </MWDProfileRule>
        <MWDProfileRule>
            <Name>Private</Name>
               <PolicyStore>universitetas.local\Windows Defender aktyvavimo politika</PolicyStore>
            <AllowLocalFirewallRules>False</AllowLocalFirewallRules>
            <AllowUserApps>False</AllowUserApps>
            <AllowUserPorts>False</AllowUserPorts>
            <Enabled>True</Enabled>
        </MWDProfileRule>
        <MWDProfileRule>
            <Name>Public</Name>
               <PolicyStore>universitetas.local\Windows Defender aktyvavimo politika</PolicyStore>
            <AllowLocalFirewallRules>False</AllowLocalFirewallRules>
            <AllowUserApps>False</AllowUserApps>
            <AllowUserPorts>False</AllowUserPorts>
            <Enabled>True</Enabled>
        </MWDProfileRule>
    </Rules>
    <ValidationFunction>Get-NetFirewallProfile</ValidationFunction>
    <EnforcementFunction>Set-NetFirewallProfile</EnforcementFunction>
</Policy>
```

5.

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy>
     <Description>Komunikacija 80 (HTTP) ir 443 (HTTPS) prievadais leidžiama visiems domeno Lietuvos
     padalinio kompiuteriams.</Description>
    <PolicyID>5</PolicyID>
    <RuleType>MWDTrafficRule</RuleType>
    <GroupPolicyName>HTTP ir HTTPS politika</GroupPolicyName>
    <ApplyTo>
            <DistinguishedName>OU=Kompiuteriai,OU=Lietuvos
            Padalinys,DC=universitetas,DC=local</DistinguishedName>
    </ApplyTo>
    <Rules>
        <MWDTrafficRule>
            <Name>{d05a9d62-6fdc-455a-a45b-debb909db81b}</Name>
            <Profile>Any</Profile>
               <PolicyStore>universitetas.local\HTTP ir HTTPS politika</PolicyStore>
            <DisplayName>Leisti įeinanti tinklo srautą 80 prievadu
               (HTTP)</DisplayName>
            <Direction>Inbound</Direction>
            <Protocol>TCP</Protocol>
            <Program>All</Program>
            <LocalAddress>Any</LocalAddress>
            <RemoteAddress>Any</RemoteAddress>
            <LocalPort>80</LocalPort>
            <RemotePort>Any</RemotePort>
            <Action>Allow</Action>
            <Enabled>True</Enabled>
        </MWDTrafficRule>
        <MWDTrafficRule>
            <Name>{cb786ce2-9b10-4a8f-a8ae-570f786b4ad1}</Name>
            <Profile>Any</Profile>
            <PolicyStore>universitetas.local\HTTP ir HTTPS
               politika</PolicyStore>
            <DisplayName>Leisti įeinanti tinklo srautą 443 prievadu
               (HTTPS)</DisplayName>
            <Direction>Inbound</Direction>
            <Protocol>TCP</Protocol>
            <Program>All</Program>
            <LocalAddress>Any</LocalAddress>
            <RemoteAddress>Any</RemoteAddress>
            <LocalPort>443</LocalPort>
            <RemotePort>Any</RemotePort>
            <Action>Allow</Action>
            <Enabled>True</Enabled>
        </MWDTrafficRule>
    </Rules>
    <ValidationFunction>Get-NetFirewallRule</ValidationFunction>
    <EnforcementFunction>New-NetFirewallRule</EnforcementFunction>
</Policy>
```

6.

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy>
     <Description>Tinklo prieiga prie buhalterinės apskaitos Microsoft SQL serverio (IP adresas -
     192.168.8.3) TCP 1433, 1434, 4022, 135 ir UDP 1434 prievadų leidžiama tik iš buhalterijos
     (192.168.7.0/24), IT (192.168.2.0/24) ir taikomųjų programų (192.168.9.0/24)
     potinklių.</Description>
    <PolicyID>6</PolicyID>
    <RuleType>MWDTrafficRule</RuleType>
    <GroupPolicyName> Prieigos prie buhalterijos duomenų serverio
    politika </GroupPolicyName>
    <ApplyTo>
         <DistinguishedName>OU=Kompiuteriai,OU=Lietuvos
         Padalinys,DC=universitetas,DC=local</DistinguishedName>
    </ApplyTo>
    <Rules>
        <MWDTrafficRule>
            <Name>{f91cf634-771a-4485-8dee-2901e36ef474}</Name>
            <Profile>Domain</Profile>
            <PolicyStore>universitetas.local\Prieigos prie buhalterijos duomenų
               serverio politika</PolicyStore>
            <DisplayName>Leisti prieigą prie buhalterijos Microsoft SQL duomenų
               serverio TCP 1433, 1434, 4022, 135 prievadų buhalterijos skyriaus
               potinkliui.</DisplayName>
            <Direction>Inbound</Direction>
            <Protocol>TCP</Protocol>
            <Program>Any</Program>
            <LocalAddress>192.168.8.3</LocalAddress>
```

```
            <RemoteAddresses>
                <RemoteAddress>192.168.2.0/255.255.255.0</RemoteAddress>
                <RemoteAddress>192.168.7.0/255.255.255.0</RemoteAddress>
                <RemoteAddress>192.168.9.0/255.255.255.0</RemoteAddress>
            </RemoteAddresses>
            <LocalPorts>
                <LocalPort>1433</LocalPort>
                <LocalPort>1434</LocalPort>
                <LocalPort>4022</LocalPort>
                <LocalPort>135</LocalPort>
            </LocalPorts>
            <RemotePort>Any</RemotePort>
            <Action>Allow</Action>
            <Enabled>True</Enabled>
        </MWDTrafficRule>
        <MWDTrafficRule>
            <Name>{b40d9b28-8833-4061-a0e6-4d2b5bb0fe9d}</Name>
            <Profile>Domain</Profile>
            <PolicyStore>universitetas.local\Prieigos prie buhalterijos duomenų
               serverio politika</PolicyStore>
            <DisplayName>Leisti prieigą prie buhalterijos Microsoft SQL duomenų
               serverio UDP 1434 prievado buhalterijos skyriaus potinkliui.</DisplayName>
            <Direction>Inbound</Direction>
            <Protocol>UDP</Protocol>
            <Program>Any</Program>
            <LocalAddress>192.168.8.3</LocalAddress>
            <RemoteAddresses>
                <RemoteAddress>192.168.2.0/255.255.255.0</RemoteAddress>
                <RemoteAddress>192.168.7.0/255.255.255.0</RemoteAddress>
                <RemoteAddress>192.168.9.0/255.255.255.0</RemoteAddress>
            </RemoteAddresses>
            <LocalPort>1434</LocalPort>
            <RemotePort>Any</RemotePort>
            <Action>Allow</Action>
            <Enabled>True</Enabled>
        </MWDTrafficRule>
    </Rules>
    <ValidationFunction>Get-NetFirewallRule</ValidationFunction>
    <EnforcementFunction>New-NetFirewallRule</EnforcementFunction>
</Policy>
```

7.

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy>
     <Description>Tinklo prieiga prie klientų duomenų Microsoft SQL serverio (IP adresas -
     192.168.8.2) TCP 1433, 1434, 4022, 135 ir UDP 1434 prievadų leidžiama iš visų skyrių
     potinklių.</Description>
    <PolicyID>7</PolicyID>
    <RuleType>MWDTrafficRule</RuleType>
    <GroupPolicyName>Prieigos prie klientų duomenų serverio
    politika</GroupPolicyName>
    <ApplyTo>
         <DistinguishedName>OU=Kompiuteriai,OU=Lietuvos
         Padalinys,DC=universitetas,DC=local</DistinguishedName>
    </ApplyTo>
    <Rules>
        <MWDTrafficRule>
            <Name>{59b9b38b-57a2-4acd-8180-aebb62f7bf81}</Name>
            <Profile>Domain</Profile>
            <PolicyStore>universitetas.local\Prieigos prie klientų duomenų
               serverio politika</PolicyStore>
            <DisplayName>Leisti prieigą prie Microsoft SQL klientų duomenų
               serverio TCP 1433, 1434, 4022, 135 visų skyrių potinkliams.</DisplayName>
            <Direction>Inbound</Direction>
            <Protocol>TCP</Protocol>
            <Program>Any</Program>
            <LocalAddress>192.168.8.2</LocalAddress>
            <RemoteAddress>Any</RemoteAddress>
            <LocalPorts>
                <LocalPort>1433</LocalPort>
                <LocalPort>1434</LocalPort>
                <LocalPort>4022</LocalPort>
                <LocalPort>135</LocalPort>
            </LocalPorts>
            <RemotePort>Any</RemotePort>
            <Action>Allow</Action>
            <Enabled>True</Enabled>
        </MWDTrafficRule>
```

```
        <MWDTrafficRule>
            <Name>{30143930-8897-4cd6-80a6-ee699dce7ccf}</Name>
            <Profile>Domain</Profile>
            <PolicyStore>universitetas.local\Prieigos prie klientų duomenų
               serverio politika</PolicyStore>
            <DisplayName>Leisti prieigą prie Microsoft SQL klientų duomenų
               serverio UDP 1434 visų skyrių potinkliams.</DisplayName>
            <Direction>Inbound</Direction>
            <Protocol>UDP</Protocol>
            <Program>Any</Program>
            <LocalAddress>192.168.8.2</LocalAddress>
            <RemoteAddress>Any</RemoteAddress>
            <LocalPort>1434</LocalPort>
            <RemotePort>Any</RemotePort>
            <Action>Allow</Action>
            <Enabled>True</Enabled>
        </MWDTrafficRule>
    </Rules>
    <ValidationFunction>Get-NetFirewallRule</ValidationFunction>
    <EnforcementFunction>New-NetFirewallRule</EnforcementFunction>
</Policy>
```

8.

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy>
     <Description>Tinklo prieiga prie Microsoft Dynamics Nav Web serverio (IP adresas - 192.168.9.2)
     TCP 80, 443 prievadų leidžiama visiems skyrių potinkliams išskyrus žmogiškųjų išteklių skyriaus
     potinkliui.</Description>
    <PolicyID>8</PolicyID>
    <RuleType>MWDTrafficRule</RuleType>
    <GroupPolicyName>Prieigos prie Microsoft Dynamics Nav Web serverio
     politika</GroupPolicyName>
    <ApplyTo>
            <DistinguishedName>OU=Žmogiškųjų išteklių skyrius,OU=Kompiuteriai,OU=Lietuvos
            Padalinys,DC=universitetas,DC=local</DistinguishedName>
    </ApplyTo>
    <Rules>
        <MWDTrafficRule>
            <Name>{542eced8-1802-4776-b8bd-33b192bc50b9}</Name>
            <Profile>Domain</Profile>
            <PolicyStore>universitetas.local\Prieigos prie Microsoft Dynamics
               Nav Web serverio politika</PolicyStore>
            <DisplayName>Blokuoti prieigą prie Microsoft Dynamics Nav Web
               serverio TCP 80, 443 prievadų žmogiškųjų išteklių skyriui.</DisplayName>
            <Direction>Outbound</Direction>
            <Protocol>TCP</Protocol>
            <Program>Any</Program>
            <LocalAddress>192.168.9.2</LocalAddress>
            <RemoteAddress>192.168.3.0/255.255.255.0</RemoteAddress>
            <LocalPorts>
                <LocalPort>80</LocalPort>
                <LocalPort>443</LocalPort>
            </LocalPorts>
            <RemotePort>Any</RemotePort>
            <Action>Block</Action>
            <Enabled>True</Enabled>
        </MWDTrafficRule>
    </Rules>
    <ValidationFunction>Get-NetFirewallRule</ValidationFunction>
    <EnforcementFunction>New-NetFirewallRule</EnforcementFunction>
</Policy>
```

9.

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy>
     <Description>Ping užklausos yra leidžiamos tik iš IT skyriaus potinklio
     (192.168.2.0/24).</Description>
    <PolicyID>9</PolicyID>
    <RuleType>MWDTrafficRule</RuleType>
    <GroupPolicyName>Ping užklausų politika</GroupPolicyName>
    <ApplyTo>
        <DistinguishedName>OU=IT skyrius,OU=Kompiuteriai,OU=Lietuvos
          Padalinys,DC=universitetas,DC=local</DistinguishedName>
    </ApplyTo>
    <Rules>
        <MWDTrafficRule>
            <Name>{f80e2c03-0acf-4f42-9012-93a83c8c904c}</Name>
            <Profile>Domain</Profile>
            <PolicyStore>universitetas.local\Ping užklausų
```

```
            politika</PolicyStore>
          <DisplayName>Leisti įeinančias Ping užklausas iš IT skyriaus
            potinklio.</DisplayName>
          <Direction>Inbound</Direction>
          <Protocol>ICMPv4</Protocol>
          <Program>All</Program>
          <ICMPTypes>
              <ICMPType>0</ICMPType>
              <ICMPType>8</ICMPType>
          </ICMPTypes>
          <LocalAddress>Any</LocalAddress>
          <RemoteAddress>192.168.2.0/255.255.255.0</RemoteAddress>
          <LocalPort>443</LocalPort>
          <RemotePort>Any</RemotePort>
          <Action>Allow</Action>
          <Enabled>True</Enabled>
      </MWDTrafficRule>
  </Rules>
  <ValidationFunction>Get-NetFirewallRule</ValidationFunction>
  <EnforcementFunction>New-NetFirewallRule</EnforcementFunction>
</Policy>
```

10.

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy>
     <Description>RDP prisijungimai turi būti įgalinti visuose organizacijos
     kompiuteriuose.</Description>
  <PolicyID>10</PolicyID>
  <RuleType>ADMXRule</RuleType>
  <GroupPolicyName>RDP įgalinimo politika</GroupPolicyName>
  <ApplyTo>
         <DistinguishedName>OU=Kompiuteriai,OU=Lietuvos
         Padalinys,DC=universitetas,DC=local</DistinguishedName>
  </ApplyTo>
  <Rules>
      <ADMXRule>
          <Name>RDP įgalinimo politika</Name>
            <Key>HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
            Services</Key>
          <ValueName>fDenyTSConnections</ValueName>
          <Type>DWORD</Type>
          <Value>0</Value>
      </ADMXRule>
  </Rules>
  <ValidationFunction>Get-GPRegistryValue</ValidationFunction>
  <EnforcementFunction>Set-GPRegistryValue</EnforcementFunction>
</Policy>
```

11.

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy>
     <Description>Tinklo lygio autentifikacija turi būti įgalinta visuose organizacijos
     kompiuteriuose.</Description>
  <PolicyID>11</PolicyID>
  <RuleType>ADMXRule</RuleType>
  <GroupPolicyName>Tinklo lygio autentifikacijos politika</GroupPolicyName>
  <ApplyTo>
      <DistinguishedName>OU=Kompiuteriai,OU=Lietuvos
        Padalinys,DC=universitetas,DC=local</DistinguishedName>
  </ApplyTo>
  <Rules>
      <ADMXRule>
          <Name>Tinklo lygio autentifikacijos politika</Name>
          <Key>HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
            NT\Terminal Services</Key>
          <ValueName>UserAuthentication</ValueName >
          <Type>DWORD</Type>
          <Value>1</Value>
      </ADMXRule>
  </Rules>
  <ValidationFunction>Get-GPRegistryValue</ValidationFunction>
  <EnforcementFunction>Set-GPRegistryValue</EnforcementFunction>
</Policy>
```

12.

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy>
     <Description>RDP prisijungimai leidžiami tik iš IT skyriaus potinklio
     (192.168.2.0/24).</Description>
    <PolicyID>12</PolicyID>
    <RuleType>MWDTrafficRule</RuleType>
    <GroupPolicyName>RDP politika</GroupPolicyName>
    <ApplyTo>
         <DistinguishedName>OU=IT skyrius,OU=Kompiuteriai,OU=Lietuvos
         Padalinys,DC=universitetas,DC=local</DistinguishedName>
    </ApplyTo>
    <Rules>
        <MWDTrafficRule>
            <Name>{59782527-d966-448a-ba22-e4c41cce81ed}</Name>
            <Profile>Domain</Profile>
            <PolicyStore>universitetas.local\RDP politika</PolicyStore>
            <DisplayName>Leisti RDP sujungimus tik iš IT skyriaus
               potinklio</DisplayName>
            <Direction>Inbound</Direction>
            <Protocol>TCP</Protocol>
            <Program>Any</Program>
            <LocalAddress>Any</LocalAddress>
            <RemoteAddress>192.168.2.0/255.255.255.0</RemoteAddress>
            <LocalPort>3389</LocalPort>
            <RemotePort>Any</RemotePort>
            <Action>Allow</Action>
            <Enabled>True</Enabled>
        </MWDTrafficRule>
    </Rules>
    <ValidationFunction>Get-NetFirewallRule</ValidationFunction>
    <EnforcementFunction>New-NetFirewallRule</EnforcementFunction>
</Policy>
```

13.

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy>
     <Description>Tinklo prieiga prie nutolusio spausdintuvo leidžiama tik iš IT (192.168.2.0/24),
     žmogiškųjų išteklių (192.168.3.0/24), marketingo (192.168.4.0/24) , klientų aptarnavimo
     (192.168.5.0/24), pardavimų (192.168.6.0/24), buhalterijos (192.168.7.0/24) skyrių
     potinklių.</Description>
    <PolicyID>13</PolicyID>
    <RuleType>MWDTrafficRule</RuleType>
    <GroupPolicyName>Spausdintuvo naudojimo politika</GroupPolicyName>
    <ApplyTo>
        <DistinguishedName>OU=IT skyrius,OU=Kompiuteriai,OU=Lietuvos
          Padalinys,DC=universitetas,DC=local</DistinguishedName>
        <DistinguishedName>OU=Žmogiškųjų išteklių
          skyrius,OU=Kompiuteriai,OU=Lietuvos
          Padalinys,DC=universitetas,DC=local</DistinguishedName>
        <DistinguishedName>OU=Marketingo skyrius,OU=Kompiuteriai,OU=Lietuvos
          Padalinys,DC=universitetas,DC=local</DistinguishedName>
        <DistinguishedName>OU=Klientų aptarnavimo
          skyrius,OU=Kompiuteriai,OU=Lietuvos
          Padalinys,DC=universitetas,DC=local</DistinguishedName>
        <DistinguishedName>OU=Pardavimų skyrius,OU=Kompiuteriai,OU=Lietuvos
          Padalinys,DC=universitetas,DC=local</DistinguishedName>
        <DistinguishedName>OU=Buhalterijos skyrius,OU=Kompiuteriai,OU=Lietuvos
          Padalinys,DC=universitetas,DC=local</DistinguishedName>
    </ApplyTo>
    <Rules>
        <MWDTrafficRule>
            <Name>{68510d43-6e65-412d-8329-72a184ed599e}</Name>
            <Profile>Domain</Profile>
            <PolicyStore>universitetas.local\Spausdintuvo naudojimo
               politika</PolicyStore>
            <DisplayName>File and Printer Sharing (NB-Datagram-In)</DisplayName>
            <Direction>Inbound</Direction>
            <Protocol>TCP</Protocol>
            <Program>System</Program>
            <LocalAddress>192.168.9.4</LocalAddress>
            <RemoteAddresses>
                <RemoteAddress>192.168.2.0/255.255.255.0</RemoteAddress>
                <RemoteAddress>192.168.3.0/255.255.255.0</RemoteAddress>
                <RemoteAddress>192.168.4.0/255.255.255.0</RemoteAddress>
                <RemoteAddress>192.168.5.0/255.255.255.0</RemoteAddress>
                <RemoteAddress>192.168.6.0/255.255.255.0</RemoteAddress>
                <RemoteAddress>192.168.7.0/255.255.255.0</RemoteAddress>
            </RemoteAddresses>
```

```
        <LocalPort>138</LocalPort>
        <RemotePort>Any</RemotePort>
        <EdgeTraversalPolicy>Block</EdgeTraversalPolicy>
        <Service>Any</Service>
        <Group>@FirewallAPI.dll,-28502</Group>
        <Action>Allow</Action>
        <Enabled>True</Enabled>
    </MWDTrafficRule>
    <MWDTrafficRule>
        <Name>{dca7e0d6-ee83-4398-ae79-6f43391ba911}</Name>
        <Profile>Domain</Profile>
        <PolicyStore>universitetas.local\Spausdintuvo naudojimo
           politika</PolicyStore>
        <DisplayName>File and Printer Sharing (NB-Datagram-In)</DisplayName>
        <Direction>Inbound</Direction>
        <Protocol>UDP</Protocol>
        <Program>System</Program>
        <LocalAddress>192.168.9.4</LocalAddress>
        <RemoteAddresses>
            <RemoteAddress>192.168.2.0/255.255.255.0</RemoteAddress>
            <RemoteAddress>192.168.3.0/255.255.255.0</RemoteAddress>
            <RemoteAddress>192.168.4.0/255.255.255.0</RemoteAddress>
            <RemoteAddress>192.168.5.0/255.255.255.0</RemoteAddress>
            <RemoteAddress>192.168.6.0/255.255.255.0</RemoteAddress>
            <RemoteAddress>192.168.7.0/255.255.255.0</RemoteAddress>
        </RemoteAddresses>
        <LocalPort>138</LocalPort>
        <RemotePort>Any</RemotePort>
        <EdgeTraversalPolicy>Block</EdgeTraversalPolicy>
        <Service>Any</Service>
        <Group>@FirewallAPI.dll,-28502</Group>
        <Action>Allow</Action>
        <Enabled>True</Enabled>
    </MWDTrafficRule>
    <MWDTrafficRule>
        <Name>{29dfe60a-6503-4ec3-b85b-250e2a43f4ee}</Name>
        <Profile>Domain</Profile>
           <PolicyStore>universitetas.local\Spausdintuvo naudojimo politika</PolicyStore>
        <DisplayName>File and Printer Sharing (NB-Name-In)</DisplayName>
        <Direction>Inbound</Direction>
        <Protocol>UDP</Protocol>
        <Program>System</Program>
        <LocalAddress>192.168.9.4</LocalAddress>
        <RemoteAddresses>
            <RemoteAddress>192.168.2.0/255.255.255.0</RemoteAddress>
            <RemoteAddress>192.168.3.0/255.255.255.0</RemoteAddress>
            <RemoteAddress>192.168.4.0/255.255.255.0</RemoteAddress>
            <RemoteAddress>192.168.5.0/255.255.255.0</RemoteAddress>
            <RemoteAddress>192.168.6.0/255.255.255.0</RemoteAddress>
            <RemoteAddress>192.168.7.0/255.255.255.0</RemoteAddress>
        </RemoteAddresses>
        <LocalPort>137</LocalPort>
        <RemotePort>Any</RemotePort>
        <EdgeTraversalPolicy>Block</EdgeTraversalPolicy>
        <Service>Any</Service>
        <Group>@FirewallAPI.dll,-28502</Group>
        <Action>Allow</Action>
        <Enabled>True</Enabled>
    </MWDTrafficRule>
    <MWDTrafficRule>
        <Name>{904635e1-f32f-41e2-8534-0e5c9591eafd}</Name>
        <Profile>Domain</Profile>
           <PolicyStore>universitetas.local\Spausdintuvo naudojimo politika</PolicyStore>
        <DisplayName>File and Printer Sharing (SMB-In)</DisplayName>
        <Direction>Inbound</Direction>
        <Protocol>TCP</Protocol>
        <Program>System</Program>
        <LocalAddress>192.168.9.4</LocalAddress>
        <RemoteAddresses>
            <RemoteAddress>192.168.2.0/255.255.255.0</RemoteAddress>
            <RemoteAddress>192.168.3.0/255.255.255.0</RemoteAddress>
            <RemoteAddress>192.168.4.0/255.255.255.0</RemoteAddress>
            <RemoteAddress>192.168.5.0/255.255.255.0</RemoteAddress>
            <RemoteAddress>192.168.6.0/255.255.255.0</RemoteAddress>
            <RemoteAddress>192.168.7.0/255.255.255.0</RemoteAddress>
        </RemoteAddresses>
        <LocalPort>445</LocalPort>
        <RemotePort>Any</RemotePort>
        <EdgeTraversalPolicy>Block</EdgeTraversalPolicy>
        <Service>Any</Service>
```

```
            <Group>@FirewallAPI.dll,-28502</Group>
            <Action>Allow</Action>
            <Enabled>True</Enabled>
        </MWDTrafficRule>
        <MWDTrafficRule>
            <Name>{2f18177b-f8ed-4e2b-828e-7843873dd832}</Name>
            <Profile>Domain</Profile>
               <PolicyStore>universitetas.local\Spausdintuvo naudojimo politika</PolicyStore>
            <DisplayName>File and Printer Sharing (NB-Session-In)</DisplayName>
            <Direction>Inbound</Direction>
            <Protocol>TCP</Protocol>
            <Program>System</Program>
            <LocalAddress>192.168.9.4</LocalAddress>
            <RemoteAddresses>
                <RemoteAddress>192.168.2.0/255.255.255.0</RemoteAddress>
                <RemoteAddress>192.168.3.0/255.255.255.0</RemoteAddress>
                <RemoteAddress>192.168.4.0/255.255.255.0</RemoteAddress>
                <RemoteAddress>192.168.5.0/255.255.255.0</RemoteAddress>
                <RemoteAddress>192.168.6.0/255.255.255.0</RemoteAddress>
                <RemoteAddress>192.168.7.0/255.255.255.0</RemoteAddress>
            </RemoteAddresses>
            <LocalPort>139</LocalPort>
            <RemotePort>Any</RemotePort>
            <EdgeTraversalPolicy>Block</EdgeTraversalPolicy>
            <Service>Any</Service>
            <Group>@FirewallAPI.dll,-28502</Group>
            <Action>Allow</Action>
            <Enabled>True</Enabled>
        </MWDTrafficRule>
    </Rules>
    <ValidationFunction>Get-NetFirewallRule</ValidationFunction>
    <EnforcementFunction>New-NetFirewallRule</EnforcementFunction>
</Policy>
```