KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS

KOMPIUTERIŲ KATEDRA

Rūta Meškauskaitė

Asmens duomenų tvarkymo audito paramos sistemos sukūrimas ir tyrimas

Magistro darbas

Darbo vadovas

doc. Algimantas Venčkauskas

Kaunas, 2011

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS

KOMPIUTERIŲ KATEDRA

Rūta Meškauskaitė

Asmens duomenų tvarkymo audito paramos sistemos sukūrimas ir tyrimas

Magistro darbas

Recenzentas
doc. dr. Antanas Mikuckas
2011-06-

Vadovas
doc. A. Venčkauskas
2011-06-

Atliko
IFN-9/3 gr. stud.
Rūta Meškauskaitė
2011-05-26

Kaunas, 2011

Turinys

Lentelių sąrašas

Paveikslėlių sąrašas

ĮVADAS

Kiekvienas turi teisę į tai, kad būtų gerbiamas jo privatus ir šeimos gyvenimas, būsto neliečiamybė ir susirašinėjimo slaptumas. - Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija.[1]

Informacija apie asmens duomenis, vadinama „asmens duomenimis“, yra renkama ir naudojama įvairiais gyvenimo atvejais. Asmens duomenis yra pateikiami, kai bandoma užsiregistruoti tam tikroje svetainėje, norint atsidaryti sąskaitą banke, įsidarbinti darbovietėje ir t.t. Asmens duomenys yra duomenys pagal kuriuos galima nustatyti asmens tapatybe, tokie kaip pavardė, vardas, asmens kodas, gyvenamosios vietos adresas.[1]

Darbą su asmens duomenimis apibrėžia atitinkami standartai, LR įsakymai, ES direktyvos, kurie užtikrina naudojamų duomenų saugumą.

Asmens duomenų tvarkymo auditas yra vienas svarbiausių veiksnių užtikrinančių duomenų saugumą. Jo pagrindinė užduotis – objektyviai įvertinti esamą organizacijos (įstaigos) asmens duomenų tvarkymo saugumo atžvilgiu būseną, atlikti išsamią analizę, kurios metu būtų nustatyta tvarkomų duomenų organizacijoje saugumo padėtis.

Asmens duomenų tvarkymo saugumas yra svarbus visoms įmonėms: atliekant auditą galima greitai nustatyti saugumo lygį ir pašalinti jų trūkumus, taip užtikrinamas asmens privatumas ir apsaugoma nuo slaptų duomenų „nutekėjimo“ trečiosioms šalims. Tačiau iškyla problema dėl asmens duomenų tvarkymo audito įrankio pasirinkimo. Nėra skiriamas reikiamas dėmesys šiai sričiai. Šiuo metu sukurti įrankiai, tokie kaip Pisa, Cobit, tik siaura dalimi yra susieti su asmens duomenų sritimi.

Dėl šių priežasčių, šiuo darbu siekiama sukurti asmens duomenų tvarkymo audito įrankį, kuriuo būtų galima nustatyti ar tinkamai organizacijoje (įstaigoje) tvarkomi asmens duomenis.

Darbo metu buvo naudojama sprendimo paramos sistema, kurios pagalba identifikuojama problema, peržiūrimi reikalingi duomenys, atliekama analizė bei ieškomi tinkamiausi sprendimo būdai. Suprojektuota ir realizuota asmens duomenų tvarkymo audito paramos sistema, atlikta sukurto įrankio analizė.

1. ANALITINĖ DALIS

1.1. Asmens duomenų sąvoka

Asmens duomenų sąvoka susiformavo Jungtinėse Valstijose 1890 m. Teisininkai Warren ir Brandeis parašė konstruktyvų darbą apie asmens teisę į privatumą „teisė būti paliktam vienu“ (ang. The right to be left alone“). Išreiškė asmens teisę, kaip socialinę vertybę, kuri turi būti saugoma įstatymų ir teisėjų. [3]

Asmens duomenų apsaugos poreikis ypatingai išryškėjo 1960, 1970 metais tobulėjant IT technologijoms. 1960 m. Europos Taryba priėmė sprendimą, kuriame buvo pabrėžiamas poreikis bei reikalingumas užtikrinti teisę į asmeninės informacijos apsaugą. 1970 m. Priimtas Vokietijos Heseno žemės asmens duomenų apsaugos įstatymas[5]. Remiantis šiuo įstatymu buvo pirmą kartą bandoma sureguliuoti asmens duomenų apsaugą. Vėliau jų pavyzdžiu pasekė Švedija, JAV, Vokietija, Prancūzija, bei kitos šalys.

Europos Tarybos Konvencija (ETS Nr. 108) 1981 m. sausio 28 d. Strasbūre pasirašė nuostatą, dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu. Pagal šią Konvenciją asmens duomenys - tai informacija apie nustatytos tapatybės asmenį arba asmenį, kurio tapatybę galima nustatyti. [6]

Darbo grupė duomenų apsaugai tvarkant asmens duomenis įkurta 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvos dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo 95/46/EB 29 straipsnio pagrindu, turi patariamąjį statusą ir veikia nepriklausomai.[7]

2000 m. gruodžio 18 d. reglamentas 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo reglamentuoja asmenų asmens duomenų tvarkymą, kai juos tvarko Bendrijos institucijos ir įstaigos. [8]

Asmens duomenų apsaugos esmė - apsaugoti žmonių teises. Pagrindinis jos tikslas yra užtikrinti, kad asmens duomenys būtų apdorojami taip, kad būtų užtikrinamas žmogaus privatumas ir kitos su tuo susijusios žmogaus teisės. [9]

Asmens duomenys – bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai. [2] Asmens duomenų sąvoką apibrėžia 1996 m. Birželio 11 d. Nr. I-1374 išleistas LR įstatymas.

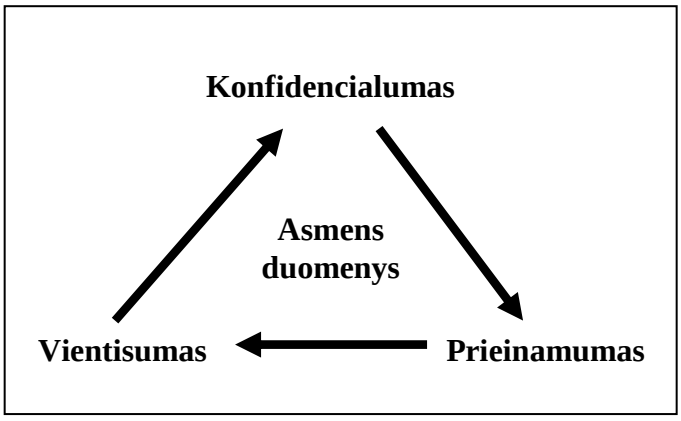
EB Duomenų apsaugos direktyva išskiria keletą asmens duomenų klasių [12]:

- Ypatingi asmens duomenys: duomenys apie rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, narystę profesinėse sąjungose, taip pat duomenys apie sveikatą ar intymų gyvenimą. Tokių duomenų tvarkymas gali būti leidžiamas tik esant išimtinėms aplinkybėms (EC direktyva, 8 str.).
- Kiti asmens duomenys: šių duomenų tvarkymas paremtas tik teisinėmis nuostatomis arba gavus duomenų subjekto sutikimą.
- Anonimizuoti arba statistiniai duomenys: šie duomenys nėra susiję su konkrečiu asmeniu ir gali būti tvarkomi be apribojimų.

Asmens duomenų tvarkymas apima veiksmus nuo jų surinkimo ir saugojimo iki persiuntimo, ištrynimo ar visiško sunaikinimo (str. EB Duomenų apsaugos direktyva).

1.2. Asmens duomenų saugumo svarba

Asmens duomenys yra vertingi, kadangi svarbūs verslo, bei kitoms organizacijoms, o svarbiausia apsaugo identifikuotą asmenį nuo neteisėto jo duomenų panaudojimo. Asmens duomenų saugumas saugo informaciją iš plataus grasinimų diapazono, kad garantuotų verslo tęstinumą, sumažintų verslo nuostolius ir maksimizuotų investicijų sugrįžimą ir verslo galimybes.



Pav. 1 Asmens duomenų saugumas naudojantis ISO/IEC 17799 standartu

Asmens duomenų saugumas susideda iš šių elementų:

a) konfidencialumas: informacija gali naudotis tik tie, kurie yra įgalioti ja naudotis.;

b) vientisumas: visuose darbo su informacija etapuose ji išlieka tos pačios originalios formos, kurią nustato jos savininkas.

c) prieinamumas: galimybė naudotis duomenimis ir informacinėmis sistemomis visada, kai to reikia, ir tiek laiko, kiek reikia. [15]

Kiekvienas juridinis subjektas, turintis įstatymo numatytą teisę tvarkyti asmens duomenis privalo pasirūpinti tų duomenų apsaugą. Duomenų apsaugą užtikrina išleistas 1996 m. birželio 11

d. Nr. I-1374 LR asmens duomenų teisinės apsaugos įstatymas, 2005 m. vasario 24 d. priimtas aktas, remiantys Europos Sąjungos sutartimi, LST ISO/IEC 17799:2005 standartas ir kt.

Vienas iš aktualiausių ir dinamiškiausiai besivystančių informacinės saugos krypčių yra informacinės saugos auditas. Kiekvienas juridinis subjektas nusprendęs atlikti asmens duomenų tvarkymo auditą, turi paruošti dokumentaciją bei informacijos saugos valdymo strategiją. Įgyvendinus šiuos reikalavimus yra atliekamas auditas.

Audito samprata - tai sisteminis objektyvių bei kokybiškų vertinimų gavimo apie informacinės saugos organizacijoje būklę procesas. Taip siekiama patikrinti įmonės situaciją, veiklą, rasti pažeidžiamas, taisytinas vietas. Auditas – tam tikras procesas, kurio metu gaunami, kaupiami, svarstomi ir vertinami objektyvūs duomenys apie asmens duomenų tvarkymo saugumo užtikrinimą. Atliktas auditas leidžia nustatyti, ar juridinio subjekto veikla atitinka audito metu nustatytus kriterijus, ar nepažeidžia teisinių reikalavimų.

Asmens duomenų tvarkymo auditą sudaro šie etapai [24]:

- Audito procedūros inicijavimas;
- Audito informacijos rinkimas;
- Audito duomenų analizė;
- Atitikimo standarto reikalavimas įvertinimas;
- Rekomendacijų paruošimas;
- Audito ataskaitos paruošimas.

Auditas būtinas norint įvertinti įmonės veiklos patikimumą, siekiant padidinti jos veiklos efektyvumą. [11] Sėkmingas audito atlikimas priklauso nuo jos metu dalyvaujančių atstovų kompetencijos, patirties, duomenų apsaugos užtikrinimo metodų. Taip pat audito proceso vykdymui turi didelę įtaką vadovybės parama, darbuotojų supažindinimas su įstaigos saugumo reikalavimais, reikiamais papildomais apmokymais.

Pagrindinis darbo tikslas – užtikrinti asmens duomenų apsaugą taikomose sistemose, padedančia išlaikyti asmeninę informaciją, apsaugoti nuo neteisėto naudojimo.

Magistrinio darbo tikslo įgyvendinimui buvo iškelti uždaviniai:

- Išnagrinėti asmens duomenų tvarkymo problemą.
- Išnagrinėti esamus asmens tapatybės nustatymo metodus.
- Atlikti esamų asmens tapatybės metodų analizę (palyginimą).
- Sudaryti savo asmens tapatybės nustatymo algoritmą.

1.3. Asmens duomenų tvarkymo saugumo problema

Kiekviena organizacija disponuoja tam tikru kiekiu informacijos. Dalis jos labai svarbi komerciniu, privatumo požiūriu, todėl jai turi būti skiriamas ypatingas dėmesys. Didžiausia problema, jog daugelis tai suvokia tik kaip fizinę apsaugą ir neskiria reikiamo dėmesio konfidencialios informacijos intelektualiai saugai. Informacijos konfidencialumą apibrėžia šie kriterijai:

- saugai naudojamos išskirtinės apsaugos priemonės;
- dėl informacijos praradimo ar neteisėto paviešinimo, organizacija gali patirti didelę žalą;
- informaciją gali naudotis tik ribotas žmonių skaičius;
- numatyta atsakomybė už neteisėtą jos atskleidimą;
- laikantys konfidencialumo nuostatomis tokią informaciją laikyti paslaptyje [22].

Nusikalstamumas yra žmonių, o ne technologijų problema. Tiesa, technologijos gali sumažinti kompiuterinių nusikaltimų paplitimą, bet esminė problema yra ta, kad žmonės gali pasinaudoti informacinių sistemų trūkumais. [14] Organizacijos darbuotojas, tiekėjas, vartotojas ir kiti, asmens duomenys gali paviešinti, perduoti tretiesiems asmenims ar piktavališkai jais pasinaudoti. Taip yra, todėl, kad žmonės ne tik kaupia informaciją, bet sugeba ją analizuoti, daryti išvadas, bei platinti. Esant palankioms sąlygoms gali tokią informaciją parduoti, suklastoti ar panaudoti savo poreikiams tenkinti. Tam, kad tokią situaciją galima būtų kontroliuoti, būtina pasirūpinti konfidencialios informacijos apsauga įmonėje.[22]

Asmens kodas yra pagrindinis identifikatorius visose viešojo sektoriaus duomenų bazėse, jo tvarkymo apribojimas neišvengiamai turės neigiamų ekonominių, teisinių bei socialinių padarinių. Nesant tikslios informacijos arba įvykus painiavai dėl netikslaus asmens identifikavimo, gali būti pažeistos paslaugomis besinaudojančių ir jomis tiesiogiai nesusijusių asmenų turtiniai ir kitokie interesai, tačiau reikia pabrėžti, kad netinkamas duomenų panaudojimas gali sukelti dar didesnę grėsmę asmeniui.

Asmens duomenų tvarkymo problema taip pat kyla dėl netinkamo ar aplaidaus duomenų vartojimo ar apdorojimo, bei sunaikinimo. Šiomis duomenų tvarkymo klaidomis gali pasinaudoti treti asmenis asmeniniams (finansiniams) tikslams.

Atskiromis duomenų subjekto teisėmis yra retai naudojamasi dėl psichologinių ir daugelio kitų priežasčių. Didesnės problemos kyla tuomet, kai trūksta informacijos apie duomenų

tvarkymo operacijas, todėl labai svarbu, kad priežiūros institucijos taip pat gintų duomenų subjekto teises (str. EB Duomenų apsaugos direktyva).[12]

Pagrindinė asmens duomenų tvarkymo problema yra duomenų tikrinimo priemonių stoka. Šiuo metu esančios audito priemonės skirtos bendram informacijos tikrinimui. Informacinės sistemos įrankis PISA apžvelgia tik siaurą sritį susijusią su asmens duomenimis, tai prieigą prie asmens duomenų, subjektams priskiriamų teisių apibrėžimą. ISO 27001 (ISO 17799) tikrina ar yra galimybė paviešinti slaptą informaciją (asmens duomenis). Be šių dar galima paminėti COBIT ir kitos. Visi šie įrankiai skirti atlikti organizacijos (įmonės) auditą, kuris apima platesnę sritį, tokią kaip rizikos, programinės įrangos saugumo įvertinimą ir kitas.

Nustatyti problemą yra ne taip paprasta. Nesupratus kylančios problemos, neteisingai suformulavus uždavinį (tikslą) sprendžiami nereikšmingi klausimai, todėl vienas pagrindinių uždavinių – teisingai kelti ir formuluoti uždavinius ir identifikuoti problemas.[18]

1.4. Asmens duomenų saugumą reglamentuojantys teisiniai aktai

Pagrindinė teisės aktų reguliuojančių asmens duomenų apsaugą prielaida - ginti žmogaus privataus gyvenimo neliečiamumo teisę, kai yra tvarkomi jo asmens duomenys, ir sudaryti sąlygas laisvam asmens duomenų judėjimui.

1.4.1. LR įstatymai

LR asmens duomenų teisiniame apsaugos įstatyme yra aprašyti visi teisiniai nutarimai, kaip reikėtų naudoti, tvarkyti, naikinti asmens duomenis. Pagrindinė teisinė dalis, apibrėžianti įmonei, kada gali naudoti subjekto asmens duomenis yra aprašyta įsakymo Nr. I-1374 nutarime.

Numatyta asmens duomenų naudojimo tvarka:

- duomenų subjektas duoda sutikimą;
- sudaroma arba vykdoma sutartis, kai viena iš šalių yra duomenų subjektas;
- pagal įstatymus duomenų valdytojas yra įpareigotas tvarkyti asmens duomenis;
- siekiama apsaugoti duomenų subjekto esminius interesus;
- įgyvendinami oficialūs įgaliojimai, įstatymais ir kitais teisės aktais suteikti valstybės bei savivaldybių institucijoms, įstaigoms ir įmonėms arba trečiajam asmeniui, kuriam teikiami asmens duomenys;

- reikia tvarkyti dėl teisėto intereso, kurio siekia duomenų valdytojas arba trečiasis asmuo, kuriam teikiami asmens duomenys, ir jei duomenų subjekto interesai nėra svarbesni. [2]

1.4.2. Europos Tarybos konvencija

1981 m. Europos Tarybos Konvencijos tikslas - ginti žmogaus asmeninį gyvenimą, o taip pat pasikeitimą informacija už valstybės sienų. Konvenciją pasirašė beveik visos iš 40 Europos Tarybos valstybių narių ir prisiėmė įsipareigojimus dėl asmens duomenų rinkimo principų, kaupimo tikslingumo, duomenų saugumo, dokumentų patikrinimo bei kontrolieriaus atsakomybės. [12]

1.4.3. Europos Sąjunga

Europos Sąjungoje yra dvi svarbios duomenų apsaugos direktyvos [13]:

- 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo
- 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. Direktyva skirta įgyvendinti dvejopo pobūdžio tikslams – iš vienos pusės apsaugoti fizinių asmenų pagrindines teises ir laisves, o ypač jų privatumo teisę tvarkant asmens duomenis, o iš kitos pusės – nevaržyti ir nedrausti laisvo asmens duomenų judėjimo tarp valstybių narių dėl priežasčių, susijusių su asmens duomenų apsauga.[5]
- Direktyva 97/66/EC (dėl asmens duomenų tvarkymo ir privatumo apsaugos telekomunikacijų sektoriuje). Direktyva nurodo, jog valstybės narės privalo prižiūrėti atsakomybės nuostatų laikymąsi ir sankcijas, išplečia duomenų apsaugos ribas, įtraukdama juridinius asmenis ir nustato užduotį Duomenų apsaugos direktyvos 29 str. darbo grupei: išsiaiškinti problemas, kylančias taikant direktyvą 97/66/EC.
- 2002/58/EC dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje

Duomenų apsaugos direktyva suteikia asmeniui, kurio asmens duomenys yra tvarkomi, įvairias teises (10-12, 14 str.), pavyzdžiui:

- teisę į informaciją apie tvarkytoją, gavėjus ir tvarkymo operacijos tikslą
- informaciją apie duomenų rūšis
- teisę susipažinti su asmens duomenimis
- teisė į ištaisymą
- teisė į ištrynimą
- teisę stabdyti duomenų tvarkymą
- teisę prieštarauti
- kompensaciją.

1.4.4. ISO/IEC 17799 standartas

ISO/IEC 17799, informacijos saugos valdymo kodas, išdėsto gerai suformuotą kontrolių komplektą, kad atkreiptų į informacijos saugumo pavojus dėmesį. 2005 metų pabaigoje pasirodžiusiame ISO/IEC 17799 standarte yra vienuolika svarbiausių skyrių, apibrėžiančių 39 kontrolės tikslus ir 133 saugumo kontroles. “Kontrolės tikslas” yra apibrėžtas kaip pageidaujamo rezultato ar tikslo tvirtinimas, kuris bus pasiektas, įgyvendindamas kontrolės procedūras detalės viduje IT veikla. “Saugumo kontrolė” yra apibrėžta kaip politika, procedūros, praktikos ar organizacinės struktūros ketinimu aprūpinti protingą draudimą, kad verslo tikslai bus pasiekti ir kad netinkamiems įvykiams sutrukdys ar aptiks ir pataisys.

ISO/IEC 17799:2005 vienuolika pagrindinių skyrių:

- Saugumo politika - aprūpina nurodymus ir vadybos patarimą tam, kad pagerintų informacijos saugumą.
- Informacijos saugumo organizavimas - lengvina informacijos saugumo vadybą organizacijos viduje.
- Turto valdymas - atlieka inventorių vertingų dalykų ir saugo šituos vertingus dalykus efektyviai.
- Žmogaus išteklių saugumas - mažina žmogaus klaidos, vagystės, apgaulės ar įžeidžiančio įrangos naudojimo pavojus.
- Fizinis ir aplinkos saugumas - trukdo pažeidimui, blogėjimui ar pramoninių patogumų ir duomenų žlugdymui.

- Komunikacijos ir operacijų vadyba - garantuoja tinkamą ir patikimą informacijos apdorojimo prietaisų operaciją.
- Prieigos kontrolė - kontroliuoja prieigą prie informacijos.
- Informacijos sistemų įsigijimas, išsivystymas ir palaikymas - garantuoja, kad saugumas yra įtrauktas į informacijos sistemas.
- Informacijos saugumo incidento vadyba - apibrėžia planą vaidinti, kai incidentai įvyksta ir trikdo teisingą apsaugos sistemos operaciją.
- Verslo tęstinumo vadyba - mažina poveikį verslo pertraukimo ir saugo kompanijos būtinus procesus nuo nesėkmės ir pagrindinės katastrofos.
- Sutikimas - vengia bet kokio pažeidimo baudžiamosios teisės ar civilinės teisės, statutinių ar sutartinių reikalavimų, ir saugumo reikalavimų. [17]

1.5. LST ISO/IEC 27001:2006 standartas

Šis tarptautinis standartas apima visus organizacijų tipus (pavyzdžiui, komercines įmones, valstybines institucijas, ne pelno organizacijas). Šiame tarptautiniame standarte apibrėžiami reikalavimai, skirti dokumentais įformintos informacijos saugos valdymo sistemos (ISVS) parengimui, įgyvendinimui, naudojimui, stebėjimui, analizei, priežiūrai ir tobulinimui, atsižvelgiant į organizacijų vykdomos veiklos bendrosios rizikos kontekstą. Jame apibrėžiami saugumo valdymo priemonių, pritaikytų atskirų organizacijų ar jų dalių poreikiams, įgyvendinimo reikalavimai. ISVS skirta užtikrinti, kad, siekiant apsaugoti informacijos turtą ir įgyti suinteresuotųjų šalių pasitikėjimą, būtų pasirenkamos adekvačios ir proporcingos saugumo valdymo priemonės. Pagrindiniai dėmesio reikalaujantys veiksniai - tai personalo kompetencijos kėlimas ir techninė apsauga nuo piktybinio informacijos paviešinimo.

1.6. Asmens duomenų valdytojo pareigos

Duomenų valdytojo (tai – viešojo arba privataus sektoriaus fizinis arba juridinis asmuo, atsakingas už asmens duomenų tvarkymą, pavyzdžiui: gydytojas, bendrovė, sporto klubas, viešoji administracija ir kt.) pareigos yra šios:

- asmens duomenis rinkti apibrėžtais ir teisėtais tikslais, nustatytais prieš renkant asmens duomenis, ir paskui tvarkomi su šiais tikslais suderintais būdais;
- asmens duomenis tvarkyti tiksliai, sąžiningai ir teisėtai;
- asmens duomenys turi būti tikslūs ir, jei reikia dėl asmens duomenų tvarkymo, nuolat atnaujinami; netikslūs ar neišsamūs duomenys turi būti ištaisyti, papildyti, sunaikinti arba sustabdytas jų tvarkymas;
- asmens duomenys turi būti tapatūs, tinkami ir tik tokios apimties, kuri būtina jiems rinkti ir toliau tvarkyti;
- asmens duomenys turi būti saugomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, negu to reikia tiems tikslams, dėl kurių šie duomenys buvo surinkti ir tvarkomi.

Asmens duomenys, surinkti kitais tikslais, gali būti tvarkomi statistikos, istoriniais ar mokslinio tyrimo tikslais tik įstatymų nustatytais atvejais, kai įstatymuose nustatytos tinkamos duomenų apsaugos priemonės.

Duomenų valdytojas gali tvarkyti asmens duomenis, jei:

- duomenų subjektas duoda sutikimą;
- sudaroma arba vykdoma sutartis, kai viena iš šalių yra duomenų subjektas;
- pagal įstatymus duomenų valdytojas yra įpareigotas tvarkyti asmens duomenis;
- siekiama apsaugoti duomenų subjekto esminius interesus;
- įgyvendinami oficialūs įgaliojimai, suteikti valstybės bei savivaldybių institucijoms arba trečiajam asmeniui, kuriam teikiami asmens duomenys;
- reikia tvarkyti dėl teisėto intereso, kurio siekia duomenų valdytojas arba trečiasis asmuo, kuriam teikiami asmens duomenys, ir jei duomenų subjekto interesai nėra svarbesni.

Draudžiama tvarkyti ypatingus asmens duomenis (duomenys, susiję su fizinio asmens rasine ar etnine kilme, politiniais, religiniais, filosofiniais ar kitais įsitikinimais, naryste profesinėse sąjungose, sveikata, lytiniu gyvenimu, taip pat informacija apie asmens teistumą), išskyrus atvejus, kai:

- duomenų subjektas duoda sutikimą;
- toks tvarkymas yra būtinas darbo ar valstybės tarnybos tikslu duomenų valdytojo teisėms ir prievolėms darbo teisės srityje įgyvendinti įstatymų nustatytais atvejais;

- reikia apsaugoti duomenų subjekto arba kito asmens esminius interesus, kai duomenų subjektas nepajėgia duoti sutikimo dėl fizinės negalios arba yra neveiksnus;
- asmens duomenis tvarko savo veikloje fondas, asociacija ar kita ne pelno organizacija politiniais, filosofiniais, religiniais ar su profesinėmis sąjungomis susijusiais tikslais, jei tvarkomi asmens duomenys yra susiję tiktai su šios organizacijos nariais arba su asmenimis, kurie nuolat kitaip dalyvauja jos veikloje dėl šios organizacijos siekiamų tikslų. Šie asmens duomenys negali būti teikiami trečiajam asmeniui be duomenų subjekto sutikimo;
- duomenų subjektas asmens duomenis paskelbė viešai;
- įstatymų nustatytais atvejais būtina užkirsti kelią nusikalstamoms ar kitoms neteisėtoms veikoms arba būtina jas tirti;
- jie yra reikalingi bylai nagrinėti teisme.

Duomenų valdytojas privalo sudaryti sąlygas duomenų subjektui įgyvendinti Asmens duomenų teisinės apsaugos įstatyme numatytas teises:

- žinoti apie savo asmens duomenų tvarkymą;
- susipažinti su savo asmens duomenimis ir kaip jie yra tvarkomi;
- reikalauti ištaisyti, sunaikinti savo asmens duomenis arba sustabdyti, išskyrus saugojimą, savo asmens duomenų tvarkymo veiksmus, kai duomenys tvarkomi nesilaikant šio ir kitų įstatymų nuostatų;
- nesutikti, kad būtų tvarkomi jo asmens duomenys.

1.7. Audito atlikimo metodai ir įrankiai

Auditas gali būti atliekamas naudojantis programine įranga arba tradiciniu būdu. Pirmuoju atveju programinės įrangos pasiūla nėra didelė, be to, turima įranga apima labai plačia saugumo sritį. Vienas iš šių įrankių yra Cobra. Ji realizuoja kiekybinius rizikų įvertinimo metodus, o taip pat konsultavimo įrankius ir saugos apžvalgos priemones. Buddy System atlieka kiekybę ir kokybinę analizę informacinėms rizikoms su fizinės saugos pažeidimais ir projektų valdymu. [14] Šios programinės priemonės dažniausiai yra paremtos ekspertinių sistemų metodika.

Kuriamos taisyklės (klausimų bazė) pagal kurias ieškomos audito metu gautos išvados (išvadų bazė) bei galimi sprendimo būdai (sprendimų bazė).

Tradicinis metodas atliekamas pačiam asmeniui (auditoriui) peržiūrint dokumentus, analizuojant esamą padėtį, pateikiant išvadas, bei ieškant galimus sprendimo būdus.

Bet kuriuo atveju auditorius, rinkdamas audito įrodymus, informaciją turi išanalizuoti audituotino objekto dokumentus. Tikrinimas atliekamas dviem būdais: dokumentiniu ir natūriniu. Taipogi reikia nuspręsti kokia tvarka (chronologine ar sistemine) bei kokiu metodu (formaliuoju ar palyginimo) bus tikrinami dokumentai. Šiuo atveju labiausiai tinkantis yra formalusis metodas, kuris nustato ar su asmens duomenimis tvarkomų dokumentų naudojimas atitinka visus keliamus reikalavimus. Palyginimo metodas daugiau skirtas su finansų tvarkymu susijusiu auditu.

Taikant stebėjimo procedūrą, yra stebimi veiksmai, kuriuos atlieka audituojamo subjekto darbuotojai. Tokiu būdu auditorius turi galimybę nustatyti realią situaciją, slypinčią už patikrinimo ataskaitų. Jis gali pateikti aiškesnį esminių problemų vaizdą, kurį galima palyginti su tuo, kaip darbuotojai vykdo dokumentuose esamus asmens duomenų tvarkymo saugumo nurodymus.

Apklausa gali būti atlikta pateikus klausimus raštu arba pokalbio metu. Klausimai gali būti aprašomieji, tikslinamieji, vertinamieji. Aprašomieji klausimai yra skirti surinkti dar nežinomai informacijai, pvz., kas ir kaip atsakingas už asmens duomenų tvarkymo saugumą. Tikslinamieji klausimai yra skirti atskirų jau žinomų faktų sutikrinimui. Vertinamieji klausimai, tai klausimai, kuriais siekiama gauti papildomos, paprastai techninės, informacijos ir išplėsti vidaus auditoriaus žinias apie specifinius procesus.

Audito metu tarp formuluojamų klausimų neturėtų būti:

- daugialypių klausimų – tai įrodo, kad auditorius nežino audituojamojo klausimo esmės;
- nukreipiamųjų klausimų – auditorius gali gauti į juos atsakymus, bet vargu ar jie tiksliai apibūdins audituojamojo klausimo esmę, nes audituojamasis patiria iš auditoriaus tam tikrą spaudimą arba nurodymą, kaip klausimas turi būti atsakytas;
- neaiškių ar tuščių klausimų, kurie neduos naudos, jeigu tiksliai nebus susieti su audituojamuoju objektu;
- hipotetinių klausimų, kadangi jie duos tik hipotetinius atsakymus, kurie negali būti naudojami kaip audito įrodymas.

Galbūt efektyviausias audito metodas yra tiesioginio stebėjimo metodas. Tai reiškia, kad auditorius stebi ir realiai mato visą procesą. Pavyzdžiui, ar gauti asmens duomenis nėra viešinami.[25]

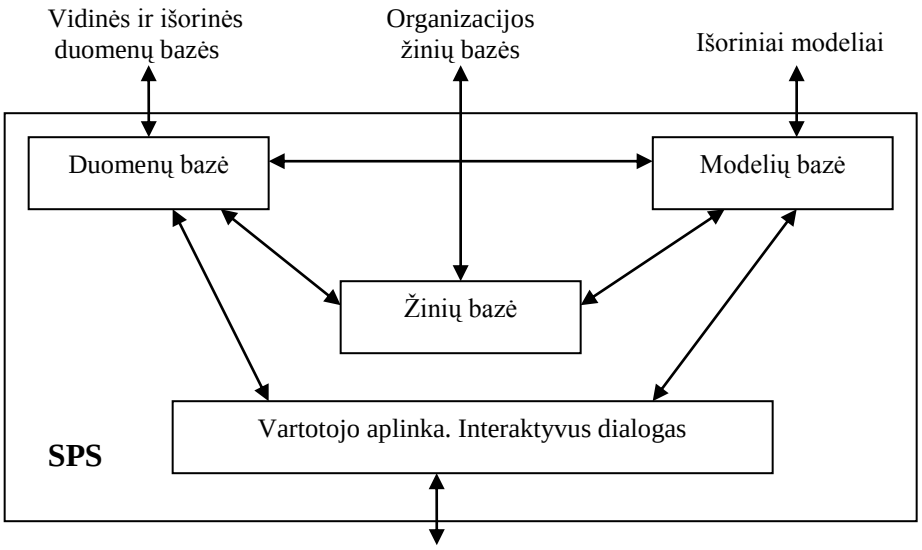
1.8. Sprendimo paramos sistema

1.8.1. Sprendimų paramos sistemos samprata

Sprendimų paramos sistema - tai informacinė sistema, kuri kaupia duomenis ir žinias iš įvairių šaltinių, juos apdoroja; naudodama įvairius matematinius ir loginius modelius, sprendimų priėmėjui teikia informaciją, reikalinga galimų sprendimų alternatyvoms analizuoti, sudaryti ir įvertinti, priimti sprendimą, gautus rezultatus išvesti ir saugoti. Taigi sprendimų paramos sistema, galinti remtis įvairių šaltinių duomenimis, turi leisti vartotojams transformuoti milžinišką neapdorotą duomenų kiekį į sprendžiamos problemos analizei ir sprendimo priėmimui nereikalingus informacinius pranešimus. [19]

J.Adomaičio teigimu[20], pagrindines sprendimo sistemos sudedamąsias dalis sudaro:

- Duomenų SPS. Šios sistemos apima duomenų apdorojimo sistemas, informacines vadybos sistemas, intelektines verslo sistemas. Duomenų SPS teikia priėjimą prie struktūrinių įmonės duomenų, taip pat leidžia juos tvarkyti.
- Modelių SPS. Sistemos, naudojančios skaičiavimo, finansų, optimizavimo modelius. Paprasčiausios modelių SPS turi statistinių ar analitinių skaičiavimų įrankius. Modelių SPS naudoja duomenis, kad padėtų sprendimų priėmėjams analizuojant situaciją.
- Žinių SPS. Tai ekspertinės sistemos. Tokios sistemos siūlo, rekomenduoja sprendėjui konkretų problemos sprendimą.
- Vartotojo sąsaja ir dialogo valdymo sistema realizuoja sprendimo priėmėjo ir SPS sąveiką ir pateikia rezultatus bei išvadas įvairių formatų (tekstiniu, skaitiniu, grafiniu, animuotu ir kt.) pavidalu.

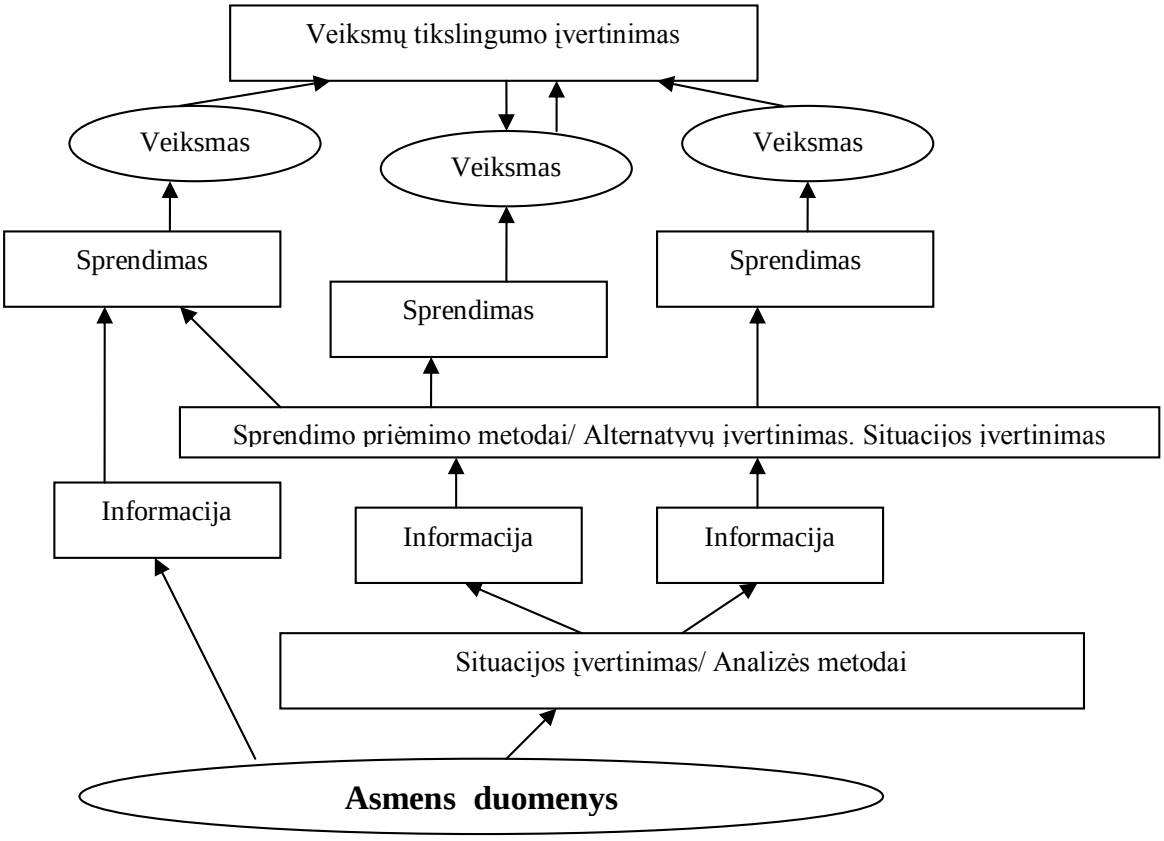


Pav. 2 SPS tipinė struktūra (komponentai ir ryšiai tarp jų) [21]

Sprendimų paramos sistemoje esantys duomenys yra labai reikšmingi, kadangi jais remiantis yra priimami sprendimai. Kuo išsamesni duomenys yra sukaupti apie nagrinėjamą objektą, tuo efektyvesnį sprendimą galima priimti [19].

Sprendimų priėmimas yra informacinis procesas, todėl visi jo etapai nuo tikslų nustatymo iki jų įgyvendinimo pabaigos ir pasekmių įvertinimo pagrįsti reikalingų duomenų paieška, vaizdavimu, apdorojimu ir analize.[19]

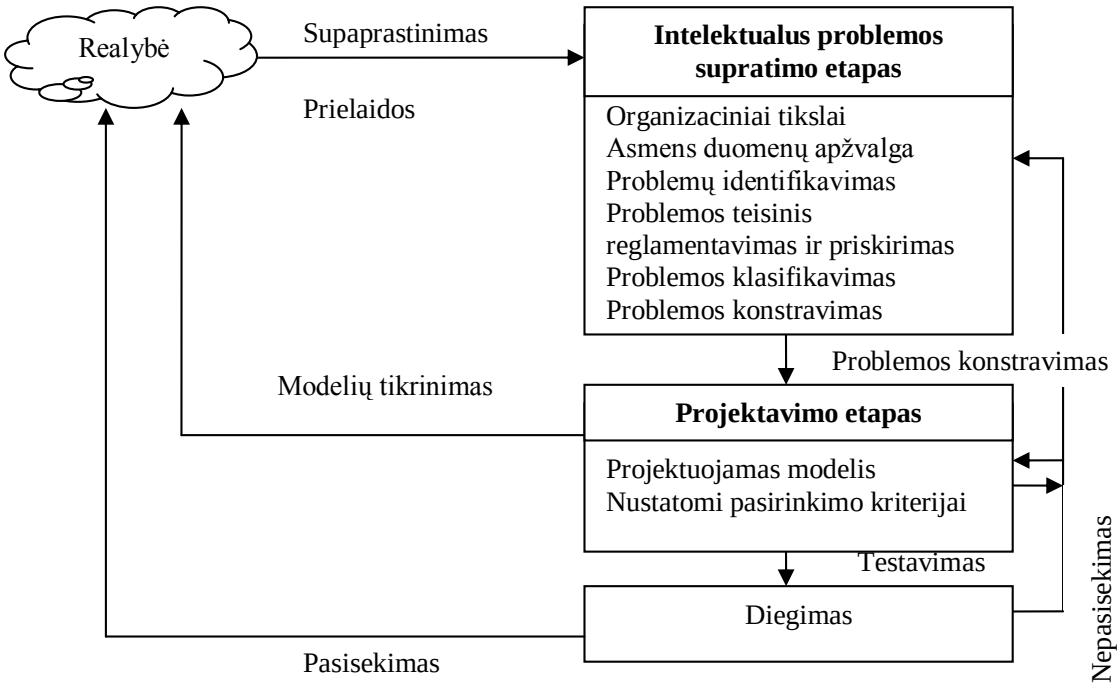
Veiksmai organizacijoje priklauso nuo sprendimo priėmimo procesų rezultatų atitinkamu organizacijos valdymo lygiu ir yra priklausomi nuo keliamų tos organizacijos veiklos tikslų. [18]



Pav. 3 Asmens duomenų, informacijos, sprendimų ir veiksmų tarpusavio ryšys organizacijoje. [18]

Sprendimo priėmimo procese pirmiausia identifikuojama problema ir jos struktūra, peržiūrimi reikalingi duomenys. Vėliau analizuojami kiti galimi problemos sprendimo modeliai. Specifiniai veiksmų atlikimo variantai koreliuojami su šiais modeliais. Analizuojami galimi sprendimo būdai. Kitame etape taikant operacijų tyrimo metodus, subjektyvaus ir intuityvaus pasirinkimo veiksnius iš galimų alternatyvių sprendinių aibės išrenkamas ir įgyvendinamas optimalus planas.[18]

Formuluojant reikalavimus sprendimų priėmimo sistemos architektūrai analizuojama keliamų problemų tipologija įmonėje arba organizacijoje, t. y. nustatomi problemų tipai, kuriems spręsti bus taikoma kompiuterinė sprendimų sistema. [18]



Pav. 4 Reikalavimai sprendimų atlikimo/ modeliavimo precesui [18]

Žemiau esančioje lentelėje pateikiami sprendimo priėmimo sistemos (SPS) privalumai ir trūkumai.

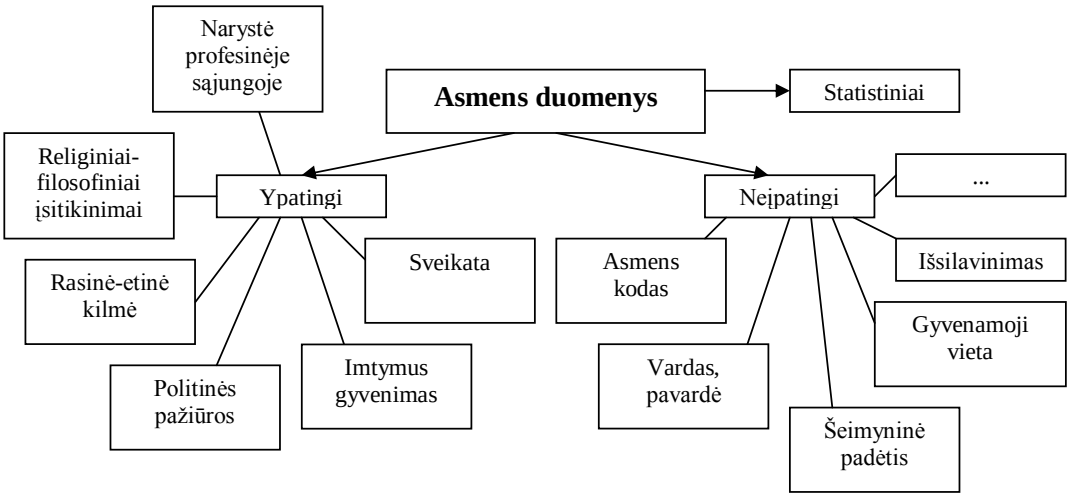
Lentelė 1 SPS privalumai ir trūkumai [26]

Privalumai	**Trūkumai / apribojimai**
Didina sprendimų priėmėjo žinių valdymo sugebėjimus	SPS nepakeičia žmogiškos patirties ir kūrybos
Leidžia sprendimų priėmėjui spręsti dideles ir kompleksines problemas	SPS įvertina tik pagal turimus duomenis duomenų ir žinių bazėje
Sprendimų priėmimą daro greitesnį ir lankstesnį	SPS veikia suprogramuotų ir įdiegtų modelių ribose.
Stimuliuoja įvairiapusišką mąstymą apie įvairius problemos sprendimo būdus	Sprendimų priėmėjai komunikuoja su SPS jos siūlomos sąsajos bei kalbos ribose
Sprendimų priėmėjas pagrįstas skaičiavimais ir analizė	
Organizacijos konkurencingumo didinimas.	

1.8.2. Duomenų bazė

Duomenų bazė(DB) - tai kartu saugomų susijusių duomenų, t. y. informacinių objektų, skirtų apdoroti kompiuteriu, visuma [19]. Duomenų sukūrimui, tvarkymui, kontroliavimui, valdymui ir naudojimui yra kuriamos duomenų bazių valdymo sistemos (DBVS), kurias sudaro

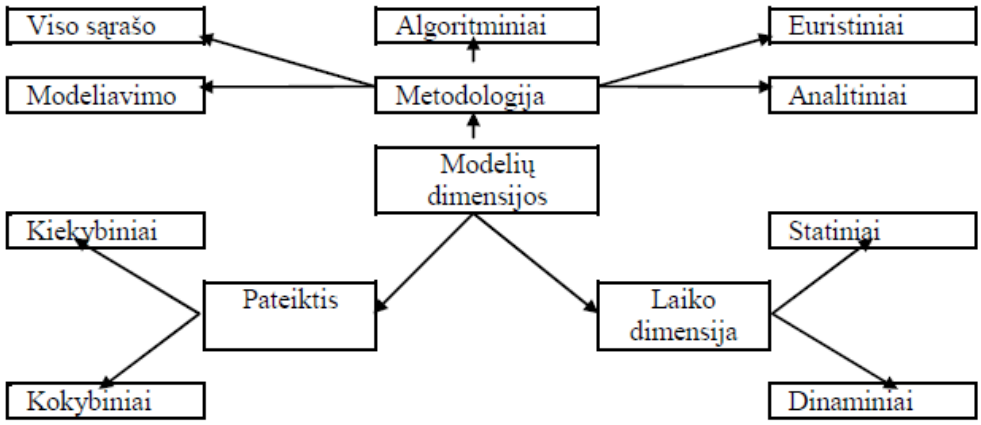
programinė įranga, atliekanti įrašymo, koregavimo, paieškos ir kitas duomenų tvarkymo funkcijas.



Pav. 5 Asmens duomenų bazė

1.8.3. Modelių bazė

Modelis - tai scheminis, abstraktus objekto esmės žymėjimas, tapačiai imituojantis jo struktūra arba jo funkcionavimą. Sprendimų paramos sistema gali apimti daug modelių. Šie modeliai gali būti tiek pačioje SPS, tiek už jos ribų. Modelius galima išreikšti trimis dimensijomis: pateiktimi, laiko dimensija ir metodologija [19].



Pav. 6 Modelių dimensijos. [19]

Pateikties modeliai. Kokybiniai modeliai remiasi subjektyviomis ekspertų nuomonėmis, patirtimi, vertinimais. Kiekybiniai modeliai atspindi objektyvias nagrinėjamų objektų savybes,

nepriklausomas nuo subjektyvių specialistų vertinimų (piniginiais vienetais, metrais, procentais ir pan.). Sprendimo priėmimo metu dažniausiai taikomi abu modeliai.

Laiko dimensijos modeliai. Statiniuose modeliuose laikoma, kad nagrinėjamos objekto savybės, laikui bėgant, nekinta. Dinaminiuose modeliuose atsižvelgiama i nagrinėjamo objekto savybių kitimą bėgant laikui.

Metodologijos modeliai. Viso sąrašo metodas taikomas surinkti ir įvertinti informaciją apie visus nagrinėjamus objektus. Algoritminiai modeliai taikomi skaičiuojant nuo pradiniu duomenų įrašymo iki ieškomo rezultato arba siekiamo tikslo gavimo. Modeliavimu sprendžiamos problemos, kuriu negalima tiksliai išnagrinėti remiantis matematine analize. Analitinio modeliavimo metu pradžioje atliekama bendra nagrinėjamo objekto analizė, o po to objektas skaidomas i dalis ir atskirai tyrinėjami sudaromieji elementai.

1.8.4. Žinių bazė

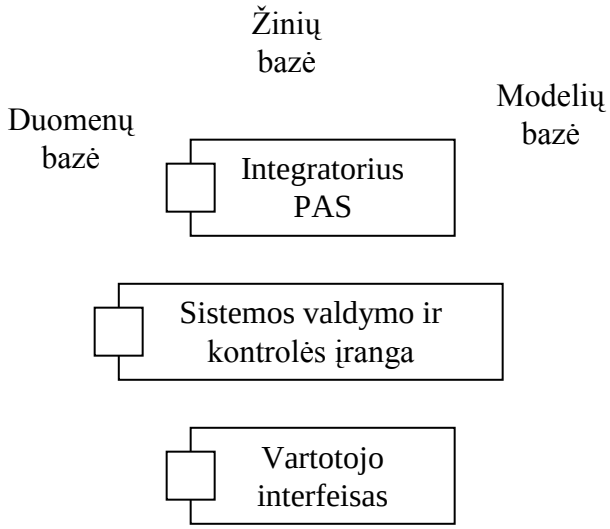
Žinių bazė - dirbtiniu intelektu paremtų taikomųjų paketų integravimas SPS architektūroje: padeda vartotojui pasirinkti adekvatų modelį/ius problemai spręsti, į matematinius modelius integruoja neapibrėžtumo ir euristikos principus, padeda vartotojui interpretuoti gautus rezultatus bei išvadas.

Žiniomis grindžiamų sistemų klasė – ekspertinės sistemos (ES). [18]

Ekspertinės sistemos sudarytos iš žinių bazės su taisyklių rinkiniu ir išvadų bei rekomendacijų pateikimo mechanizmais. Remdamosi pradiniais duomenimis ir taisyklių rinkiniais, ekspertinės sistemos atpažįsta situaciją, nustato diagnozę, suformuluoja sprendimą, rekomenduoja pasirinkti veiksmus. ES paprastai sprendžia tokius uždavinius, kuriems spręsti paprastai reikia žmonių ekspertizės. Be to, kaip ir ekspertas, ji vykdo daug antrinių funkcijų, tokių kaip klausimų uždavimas, savo samprotavimų aiškinimas, simbolinių išraiškų apdorojimas ir jų pagrindų atliekamas samprotavimas, išvadų pagrindimas ir t. t. [19]

Centrinė sprendimų paramos sistemos dalis – problemų apdorojimo sistema (PAS), kurią sudaro: duomenų bazės valdymo, teksto procesorių, modelių įvykdymą, išvedimo priemonės ir samprotavimas, elektroninių lentelių ir statistinė analizė.[18]

Dėl šių ir daugelio kitų priežasčių kyla būtinybė taikyti jose dirbtinio intelekto teorijos metodus, įtraukiant šiuos metodus į žinių ir modelių bazės komponentų struktūras.



Pav. 7 Bendroji sprendimo priėmimo sistemos komponentinė architektūra [18]

Dirbtinis intelektas – programinė įranga, imituojanti žmogaus mąstymą kompiuteryje. Tokios sistemos sukūrimui yra būtina išanalizuoti žmogaus, sprendžiančio tam tikrus uždavinius arba priimančio sprendimus tam tikroje srityje, mąstymą, išskirti pagrindinius šio proceso etapus ir sukurti programas, imituojančias šį procesą kompiuteryje. Žmogaus smegenys – didžiulė žinių saugykla. Žmogui būdinga kaupti naujas žinias ir taikyti jas įvairiose situacijose. Intelektą galima būtų apibūdinti kaip visumą faktų ir jų taikymo būdų tikslui pasiekti. Tikslai pasiekiami visų žinomų faktų taikymo taisyklių pagalba [19].

Sprendimo procesas modeliuojamas problemos sprendimo erdvėje, skaidomas į tam tikrą skaičių tipiškų procesų, atvaizduojančių įvairias problemos analizės, diagnozės, įvertinimo, tikslo prioriteto pasirinkimo fazes. Aprašomas tikslų modelis ir analizuojama jo įtaka nustatant kriterijus, kurie leistų pasirinkti naudingesnius ir patikimesnius sprendimus iš galimų alternatyvių sprendimų variantų.

Parenkant alternatyvą būtina įvertinti galimas jos realizavimo pasekmes. Alternatyva parenkama vadovaujantis vartotojo pirmenybės teikimo funkcija. Šiai funkcijai aprašyti gali būti naudojamos sprendimo priėmimo modelių bibliotekos, grindžiamos prasmingai teisingų pirmenybės teikimo funkcijų struktūros modeliais, aprašomais lyginamaisiais projektavimų atributų metodais, ir kt.[18]

1.9. Sprendimo priėmimo kriterijai

Sprendimų priėmimo taisyklės gali būti išreiškiamos per sprendimų lenteles [18]. Lentelėse yra pateikiamos sąlygos bei veiksniai, kurie lemia galutinį rezultatą. Atitinkamai pagal pateiktas sąlygas, veiksnius yra priskiriami galimi atsakymai su turimais svoriais, kurie išreiškiami procentine išraiška. Priklausomai nuo rezultato svarbumo atitinkamai suteikiama didesnė procentinė išraiška (maksimali reikšmė 100%). Žemiau pateikta sprendimų lentelė, bei pavyzdys.

Lentelė 2 spendimų lentelės bendras vaizdas

Taisyklė	Atsakymas 1	Procentinė reikšmė 1	Atsakymas 2	Procentinė reikšmė 2	...	...	Atsakymas n	Procentinė reikšmė n
Sąlyga1	T	Pr1	N	Pr2				
Sąlyga2	T	Pr1	N	Pr2				
...	..	...	..	...				
Veiksnys1	X	Pr1	X	Pr2	...	...	X	Pr m
Veiksnys2	X	...	X	...	...	...	...	...
...	...	...	...	...	...	...	...	...

T – taip, N – ne, X – taip.

Pateiktame pavyzdyje pateikta sąlyga (Ar įstaigoje yra asmens duomenų naudojimosi schema?) ir galimi tik du atsakymai (Taip arba ne). Jei patvirtinama, kad tokia saugumo schema yra, tai toliau bandoma patikslinti kokios asmens duomenų naudojimosi taisyklės šiame dokumente yra apibrėžiamos.

Lentelė 3 pateikiamas sprendimų lentelės pavyzdys

Taisyklė	Ats. 1	Proc. 1	Ats. 2	Proc. 2	Ats. 2	Proc. 3	Ats. 4	Proc. 4	Ats. 5	Proc. 5
Ar įstaigoje yra asmens duomenų naudojimosi schema?	Taip	100%	Ne	0%						
Kurie iš žemiau pateikto sąrašo yra aprašyti asmens duomenų tvarkymo saugumo taisyklėse?	Kopija-vimas	20%	Saugo-jimas	20%	El. perda-vimas	20%	Žodinis perda-vimas	20%	Sunaiki-nimas	20%

Priimant sprendimą, bei įvertinant daugelį kriterijų, kurių reikšmes galima formaliai apskaičiuoti, reikia jį įvertinti kiekybiškai.

Max F(x) esant ribojimui $x \in A \subset R^n$,

čia $x=(x_1,\ldots,x_n)$ – objektą aprašantis n komponenčių vektorius, $F(x) = (f_1(x),\ldots, f_m(x))$ - kriterijų funkcijų vektorius, m - kriterijų skaičius. Sritis A gali būti aprašoma taip:

$A = \{x : vec\_B(x) < 0\}$, $vec\_B(x) = (b_1(x), ..., b_k(x))$ yra ribojimų funkcijų vektorius, k – ribojimų skaičius. Ribojimai apibrėžia leistiną sprendimų aibę.

Galimi papildomi ribojimai: a<f(x)<b, i=1,...,m. Taip atmetamos beprasmės tyrinėti kriterijų reikšmės.

Daugelio kriterijų sprendimų priėmimas nurodo į sprendimų priėmimą keleto paprastai konfliktuojančių tikslų sąlygomis. Tokiu atveju kriterijai gali būti prieštaringi, ir negalima vienareikšmiškai atsakyti koks sprendimas yra geriausias.

Sprendimams palyginti įvedamas dominavimo veiksnys: sprendinys x_1 dominuoja sprendinio x_2 atžvilgiu, jeigu $f_i(x^1) >= f_i(x^2), j = 1,...m$ ir egzistuoja bent vienas j, kuriam $f_i(x^1) > f_i(x^2)$.

Sprendinys $y \in A$ nėra dominuojantis, jeigu nėra $x^* \in A$ tokio, kad $f_i(x^*) >= f_i(y), j = 1,...m$, ir egzistuoja bent vienas j, kad $f_i(x^*) > f_i(y)$. Toks sprendinys y vadinamas efektyviu arba Pareto – tinkamu sprendiniu[18].

Pagal surinktų taškų sumą, įvertinant asmens duomenų tvarkymo patikimumą, galutiniame sprendime sistema gali pateikti tokias bendras išvadas:

- labai gerai – jeigu asmens duomenis tvarkomi, pagal visus nustatytus reikalavimus;
- gerai – jeigu asmens duomenis tvarkomi, pagal visus nustatytus reikalavimus, išskyrus nedideles išimtis;
- vidutiniškai – jeigu asmens duomenis tvarkomi tam tikru saugumo lygiu;
- blogai - jeigu asmens duomenis tvarkomi neatsižvelgiant į nustatytus reikalavimus.[25]

1.10. Išvados

Darbo metu apžvelgta asmens duomenų sąvoka bei su jos tvarkymu susijusios kylančios problemos. Peržiūrėti LR teisiniai aktai, ES direktyvos bei ISO/IEC 17799 ir LST ISO/IEC 27001, kuriuose kalbama apie naudojamų asmens duomenų saugumą, darbuotojų patikrinimą, tai yra ar neviešina turimos informacijos, ar nenaudoja saviems piktavališkiems tikslams ir kt.

Asmens duomenų tvarkymo patikrinimas atliekamas audito pagalba. Auditas gali būti atliekamas naudojantis programine įranga arba tradiciniu būdu. Šiuo metu esamų programinės įrangos sistemų skirtų asmens duomenų tvarkymo auditui atlikti nėra. Turimos sistemos yra skirtos bendram įmonės (veiklai, saugumui, rizikos faktorių) patikrinimui atlikti, pvz.: Cobra –

realizuoja kiekybinių įvertinimo metodus ir saugos apžvalgos priemones. Šios sistemos dažniausiai pagrįstos sprendimų paramos sistemomis. Kurios kaupia duomenis ir žinias iš įvairių šaltinių, juos apdoroja, naudoja įvairius matematinius loginius modelius, sprendimų priėmėjui teikia informaciją, reikalinga galimų sprendimų alternatyvoms analizuoti, sudaryti ir įvertinti, priimti sprendimą, gautus rezultatus išvesti.

Tradicinis metodas atliekamas pačiam asmeniui (auditoriui) peržiūrint auditui atlikti reikiamus dokumentus, analizuojant esamą padėtį, pateikiant išvadas ir ieškant galimų sprendimo būdų.

Išanalizuota sprendimų paramos sistemos architektūra, jos sudedamosios dalys (žinių bazė, duomenų bazė, modelių bazė), bei nustatyti sprendimo priėmimo kriterijai. Sprendimo priėmimo taisyklės yra išreiškiamos per sprendimų lenteles. Šiose lentelėse yra pateikiamos sąlygos bei veiksniai, kurie lemia galutinį rezultatą. Atitinkamai pagal pateiktas sąlygas ir veiksnius, priskiriami galimi atsakymai su turimais svoriais.

2. PROJEKTINĖ DALIS

2.1. Tikslai

Sukurti asmens duomenų tvarkymo audito sprendimo priėmimo sistemą, kuria asmuo galėtų pasinaudoti tikrinant asmens duomenų tvarkymo saugumą įmonėje. Pagal gautus rezultatus sistema pateiktų išvadas, bei galimus sprendimus kaip gerinti duomenų tvarkymo saugumą turimoje įmonėje.

Sprendimų priėmimo sistema vartotojui pateiks atitinkamus klausimus ir pagal vartotojo (auditoriaus) pateiktus atsakymus sistema pateiks galimus spendimo būdus šalinti kylančias asmens duomenų tvarkymo saugumo spragas.

2.2. Reikalavimai sprendimų priėmimo sistemai

Sistema pagal auditoriaus pateikta informaciją turi pateikti ataskaitą apie kylančias įmonėje asmens duomenų tvarkymo saugumo problemas, bei tinkamiausius sprendimo būdus.

Minimalūs reikalavimai naudotojų programinei įrangai:

- Operacinė sistema: 2000/XP/Vista/7/Linux/Unix
- Naršyklės: Internet Explorer (6 arba vėlesnė versija), Firefox 2.x, Firefox 3.x, Opera (9.5 arba vėlesnė versija), Chrome (2.0 arba vėlesnė versija)
- Įdiegta Java Server Pages (CGI), Active Server Pages (ASP), Common Gateway Interface (SGI)

Reikalavimai programinei įrangai skirstomi į dvi grupes:

- Sistemos funkciniai reikalavimai: kokias funkcijas turi atlikti kuriama sistema, ir kaip šios funkcijos turi būti atliekamos. Šiuolaikiniai programinės įrangos kūrimo metodai paprastai siūlo funkcinius reikalavimus modeliuoti taikant panaudos atvejų metodiką.

- Nefunkciniai reikalavimai: kokybės atributai (patogumas, patikimumas, greitis, palaikomumas, saugumas), juridiniai bei kontrolės reikalavimai, palaikomos operacinės sistemos, suderinamumas ir kt.[1]

Sistemos funkciniai reikalavimai:

- Pagal vartotojų pateiktus atsakymus atrinkti tinkamiausius sprendimo būdus iškilusioms asmens duomenų tvarkymo saugumo spragoms spręsti.
- Galimybė auditoriui peržiūrėti abejotino klausimo svarbumą.
- Visi audito metu gauti duomenys turėtų būti kaupiami ir saugomi.
- Galimybė papildyti žinių bazę: kurti taisykles-klausimus, rekomendacijas.

Sistemos nefunkciniai reikalavimai:

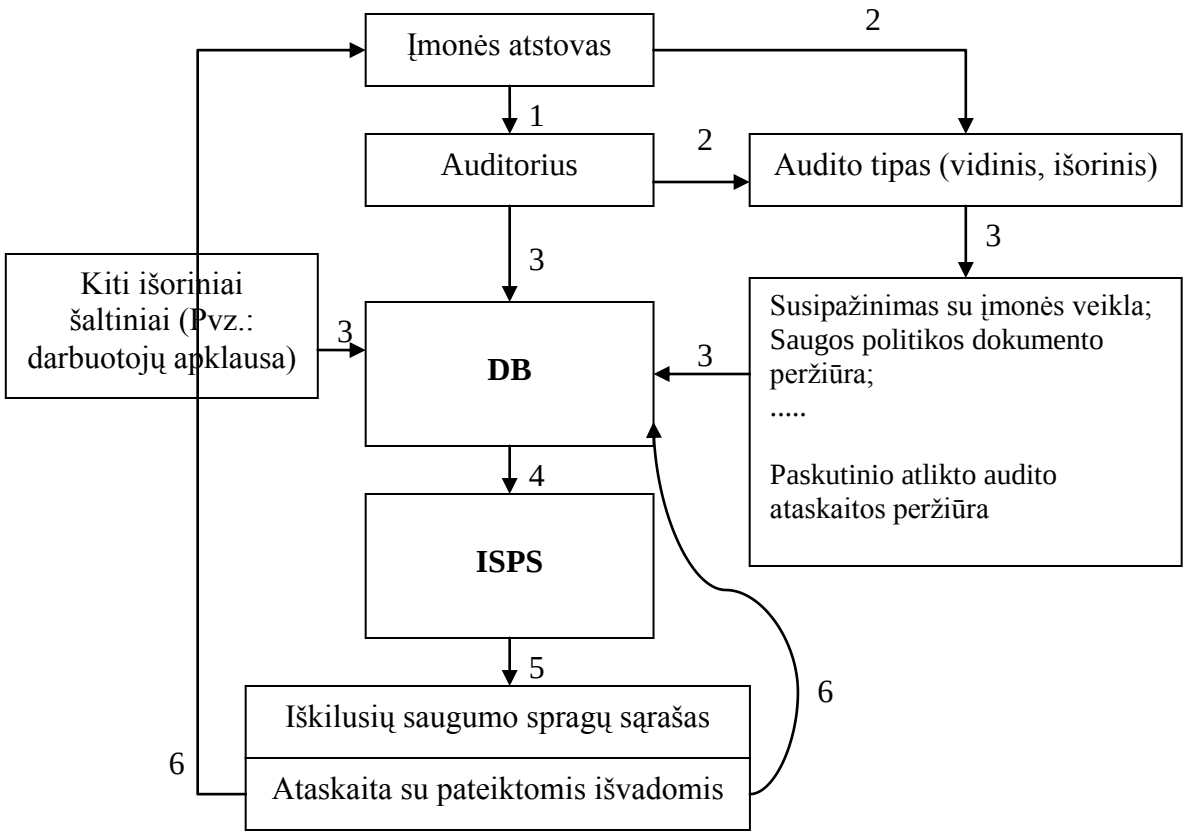
- Nesudėtinga vartotojo sąsaja.
- Lengvai suprantami vartotojui pateikiami klausimai.
- Klausimai pateikti pagal visus turimus saugumo standartus (teisinius aktus ir kt.)
- Konfidenciali informacija apsaugoma nuo nesankcionuotos prieigos arba paviešinimo;

Audito metu nustatyti faktai turi būti detaliai aprašyti skaitytojui lengvai suprantama, logiška tvarka:

- kriterijai – nurodoma kokiais standartais, priemonėmis arba lūkesčiais remtasi, atliekant įvertinimą ir/arba patikrinimą;
- būklė – faktinė padėtis, kurią auditorius nustatė tikrinimo metu;
- priežastys – nurodomos priežastys, kodėl yra skirtumų tarp tos būklės, kokia ji turėtų būti ir faktinės būklės;
- poveikis – kas atsitinka arba gali atsitikti dėl esamos būklės;
- rekomendacija – ką reikėtų daryti, kad situacija pagerėtų.

2.3. ISPS asmens duomenų tvarkymo vertinimo procese

Asmens duomenų tvarkymo vertinimo procesas ir ISPS (Intelektualios sprendimo paramos sistemos) vieta jame pavaizduoti 8 pav.:



Pav. 8 Asmens duomenų tvarkymo vertinimo procesas ir ISPS [21]

Šiame procese išskiriami 6 etapai:

1) inicijavimo etape auditorius ar jų grupė sutaria su audituojamos organizacijos atstovais organizacijoje vykdyti informacijos saugos auditą.

2) tipo parinkimas. Auditorius ir organizacijos atstovas susitaria dėl vykdomo asmens duomenų tvarkymo audito tipo pasirinkimo.

3) informacijos paieškos etape renkama informacija. Auditorius surenka pirminę informaciją iš organizacijos atstovo pateiktų duomenų (susipažinimas su įmonės veiklos, turimų dokumentų, informacijos saugos politikos ir t.t.) reikalingų auditui atlikti.

4) Naudojantis ISPS atliekama asmens duomenų tvarkymo analizė. Audito vertinimo procese analizuojami šie aspektai:

- apibrėžiami asmens duomenų tvarkymo saugumo kriterijai;
- nustatomas duomenų tvarkymo saugumo lygis;
- pateikiamas sprendimų sąrašas iškilusioms saugumo spragoms spręsti.

Analizės metu pateikiamos atlikto audito išvados.

5) priimami sprendimai pagal pateiktas išvadas, kokiomis priemonėmis ir kuriose srityse reikėtų ištaisyti kylančias saugumo spragas.

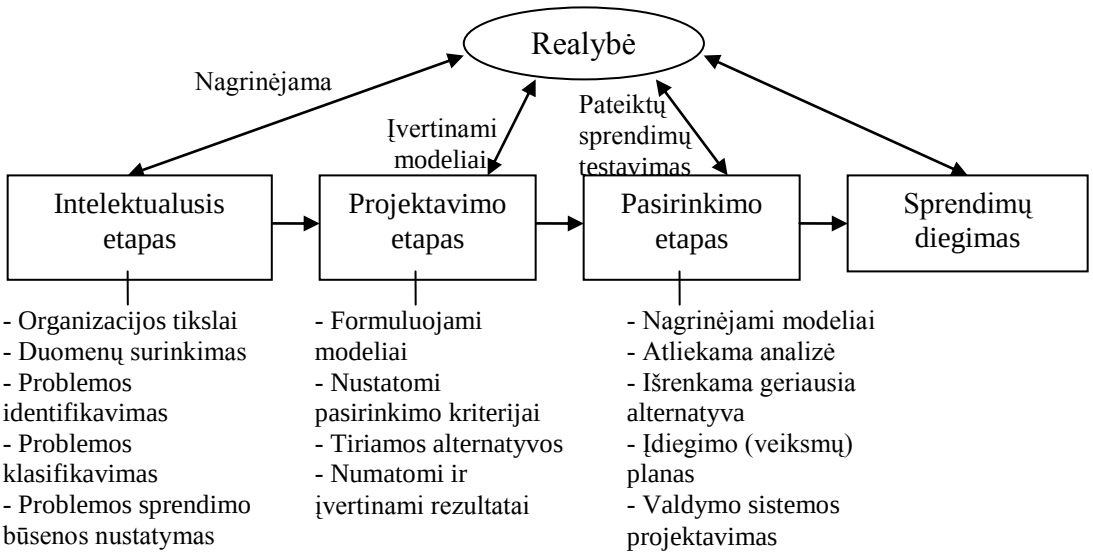
6) grįžtamasis ryšys. Šiame etape pateikiama įmonės atstovui gauta ataskaita bei papildoma gautais rezultatais duomenų bazė.

Paskutiniame etape auditorius turi patikrinti, ar trūkumai, nurodyti jo pranešime, buvo pašalinti.

2.4. Sprendimo paramos sistemos kūrimo metodika

Sprendimo priėmimo sistema vadinama sistema, parenkanti arba padedanti parinkti tam tikru požiūriu geriausią arba bent jau priimtiną alternatyvą iš jos pačios formuojamų arba jai pateiktų alternatyvų aibės ir tai padaro įvertindama galimas alternatyvos realizavimo pasekmes. [18]

Sprendimo priėmimo proceso etapai yra keturi: intelektualusis, projektavimo, pasirinkimo ir įgyvendinimo. Intelektualiajame etape nustatomi reikalingi duomenys, įvertinamas sprendimo procesas, identifikuojamos probleminės sritis, atliekama jų analizė. Projektavimo etape formuojami modeliai, tiriamos alternatyvos, nustatomi pasirinkimo kriterijai.

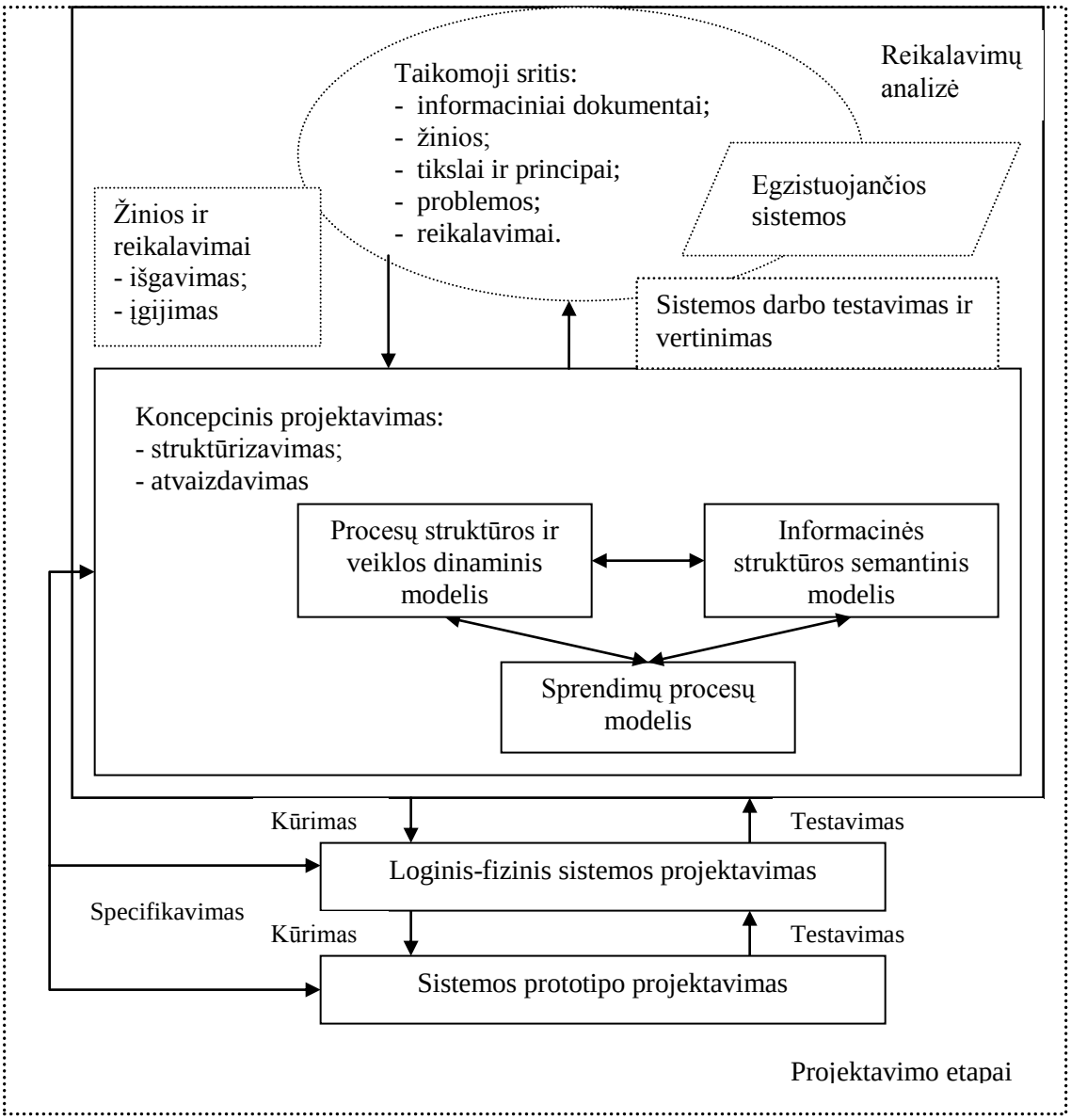


Pav. 9 Sprendimo atlikimo ir projektavimo proceso stadijos [18]

Projektavimo etapai detaliau pateikti žemiau esančioje schemoje (pav. 10).

Reikalavimų analizės etape įgyjamos žinios iš taikomosios srities specialistų, ir ekspertų. Koncepcinio modeliavimo priemonėmis jos struktūrizuojamos ir atvaizduojamos. Įvertinimo

tinklų priemonės leidžia išreikšti procesų struktūrą ir dinaminio valdymo imitavimą. Koncepcinis modelis atspindi ir taikomojoje srityje vykstančius procesus.



Pav. 10 Sprendimus palaikančios sistemos projektavimo etapai

Projekto funkcinius reikalavimus aprašanti dedamoji išraiška probleminėje srityje vykstančių procesų sąveikavimo struktūrą ir dinamiką, vidinius procesų ryšius, informacijos kaupimo taškus, galimus procesų ciklus ir kita. Šio dinaminio-imitacinio modelio sudarymo etape formuojasi informacinės bazės struktūros aprašymo reikalavimai. Statinis modelis išreiškia informacinę struktūrą, kuri atspindi semantinę išskiriamų objektų tarpusavio sąveiką.

Kitame etape įvertinimo tinklai taikomi sprendimo priėmimo procesams aprašyti. Šis daugialygis sprendimų procesų aprašymo ir valdymo modelis atvaizduoja bendrą sprendimo priėmimo strategiją, kuri apima informacinės bazės elementų sinchronizuotą tikrinimą pagal dinaminiame modelyje išskirtus kritinius taškus, nustato tiriamojo objekto einamąją būseną, šios informacijos lyginimo su normatyvine informacija eigą ir pagal šio įvertinimo rezultatą galimų alternatyvių sprendimų variantų pateikimą.

Projektuojant sprendimus leidžiančią priimti sistemą, išskiriami trys žinių atvaizdavimo lygiai: taikomosios (probleminės) srities informacijos semantikos, analizuojamos taikomosios srities veiklos ir sprendimų priėmimo procesų. Probleminės srities semantikos ypatumai atvaizduojami per statinius aspektus išreiškiantį koncepcinį modelį. Žinios yra išgaunamos kontekstinio probleminės srities supratimo būdu. Konstruojamas semantinis modelis, išreiškiantis kokybinius esmių, procesų, situacijų, jų tarpusavio ryšių ir gyvavimo ciklų bruožus. Organizaciniai probleminės srities principai atskleidžiami semantiniame statinius aspektus atvaizduojančiame modelyje.

Dinaminius aspektus išreiškiantis modelis sudaromas analizuojant pagrindinių, semantiškai svarbių informacinių vienetų veiklą, stebimą skirtingais detalumo lygiais. Dinaminių aspektų atvaizdavimo lygis parodo stebimų procesų taikomojoje srityje struktūros sąveikavimą ir jų vykdymo dinamiką. Šiame sprendimo paramos sistemos projektavimo etape apžvelgiamas semantinis informacijos, svarbios sprendimams ir išvadoms pagrįsti, išskyrimas ir įvertinimas bei informacijos pateikimo ir išvadų tvarkos formos parinkimas.

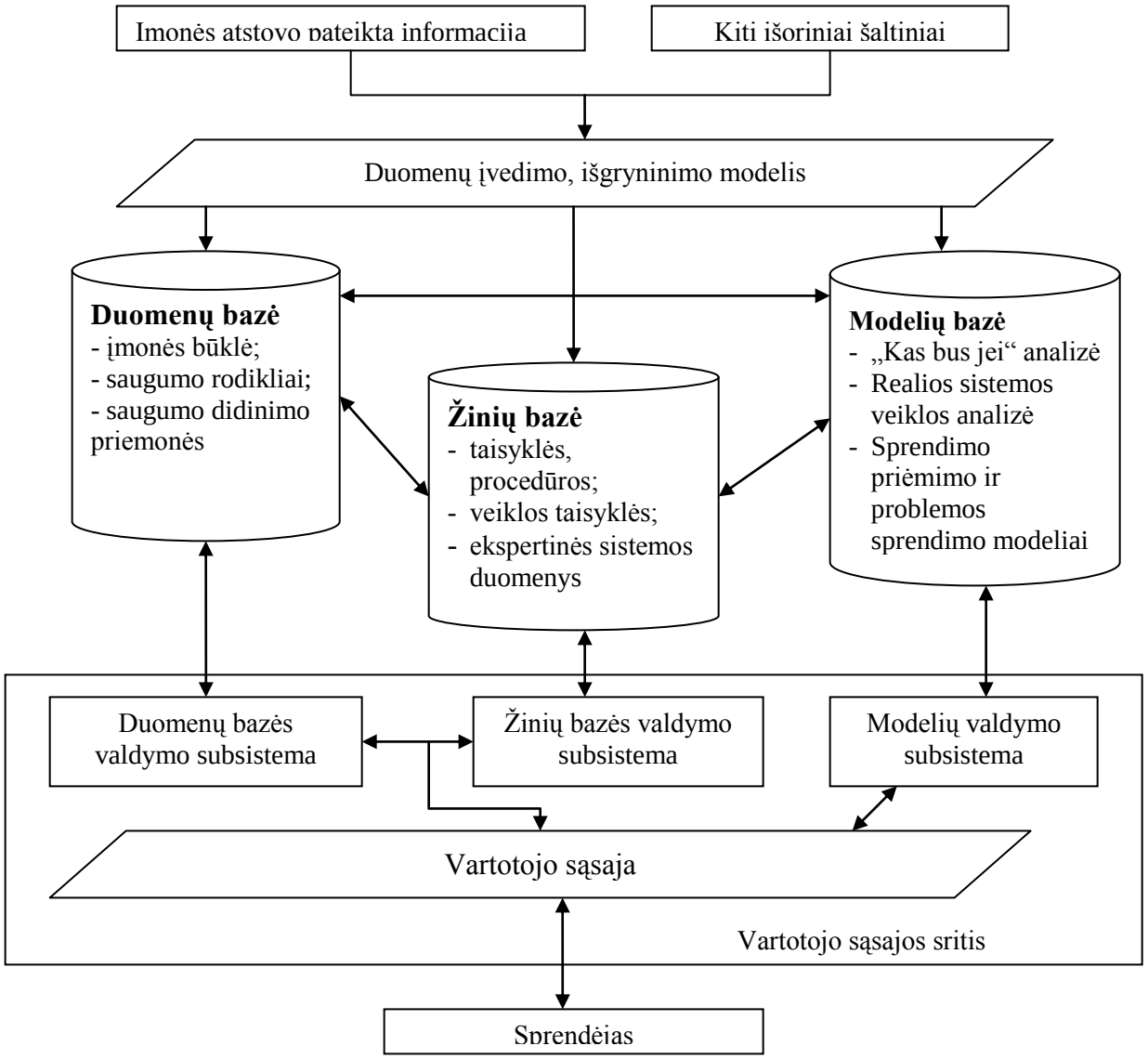
2.5. Sprendimo priėmimo sistemos architektūra

Pagal ištirtą asmens duomenų tvarkymo audito vertinimo procesą, sumodeliuotą ISPS vietą jame, taip pat pagal sukurtų ISPS tyrimų rezultatus sumodeliuojama kuriamos ISPS struktūra (architektūra), ji pateikiama pav. 8.

Šioje architektūroje realizuoti visi tipinio SPS modelio komponentai: DB, modelių bazė, žinių bazė, vartotojo sąsaja. Kiekvienoje bazėje įvardinti pagrindiniai jos taikymo metodai, turinys. Bazes vartotojo sąsajos pagalba vartotojas pasiekia per duomenų bazės, žinių bazės, modelių bazės valdymo sistemas. Bazės susijusios tarpusavyje: DB talpina duomenis, reikalingus žinių bazėje realizuotam ekspertiniam situacijos vertinimui, įvairiapusei analizei modelių bazėje. Šių analizių metu gauti rezultatai talpinami į duomenų bazę, atnaujinamos žinių bazės turinys.

Intelektualios sprendimų paramos sistemos struktūra asmens duomenų tvarkymo audito vertinimui

Sistemoje numatomas svarbiausių sprendėjui rezultatų išrinkimo (intelektualaus asistento) modulis, taip pat duomenų, surenkamų iš vidinių ir išorinių šaltinių išrinkimo ir agregavimo modulis. Informacijos šaltiniai: paskutinio audito metu gauta ataskaita ir kt.[21]

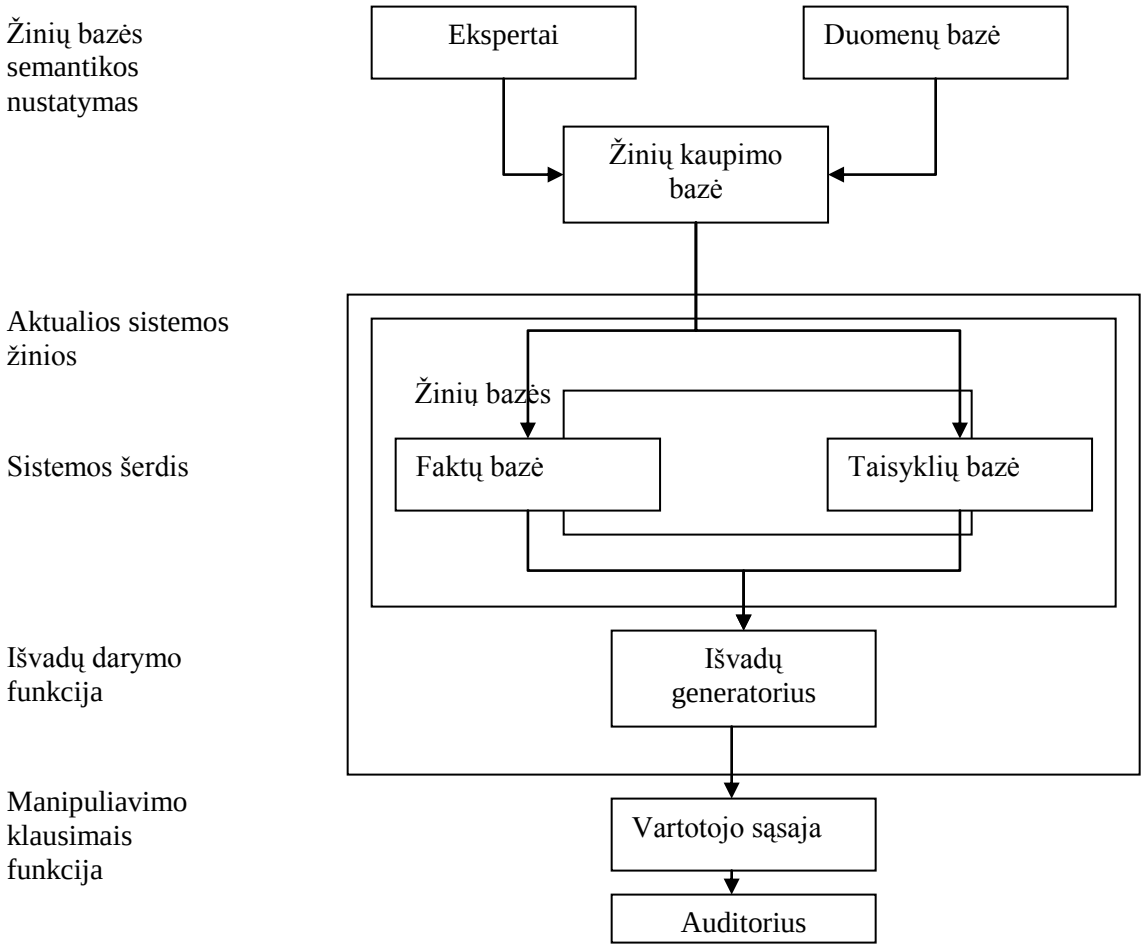


Pav. 11 Siūlomos sprendimo sistemos vertinimui architektūra

Iš aukščiau esančios architektūros schemos (pav. 11) pamėginsime akcentuoti pagrindines kuriamos sistemos dalis. Pagrindinės sprendimų paramos sistemos architektūros dalys yra šios (pav. 12):

- žinių įvedimo modulis (duomenų įvedimo, išgryninimo modelis);

- žinių bazė, kurią sudaro dvi atskiros dalys: faktų ir taisyklių bazė;
- išvadų generatorius;
- vartotojo ryšio su sistema modulis (vartotojo sąsaja).



Pav. 12 Pagrindinės sistemos architektūros sudedamosios dalys

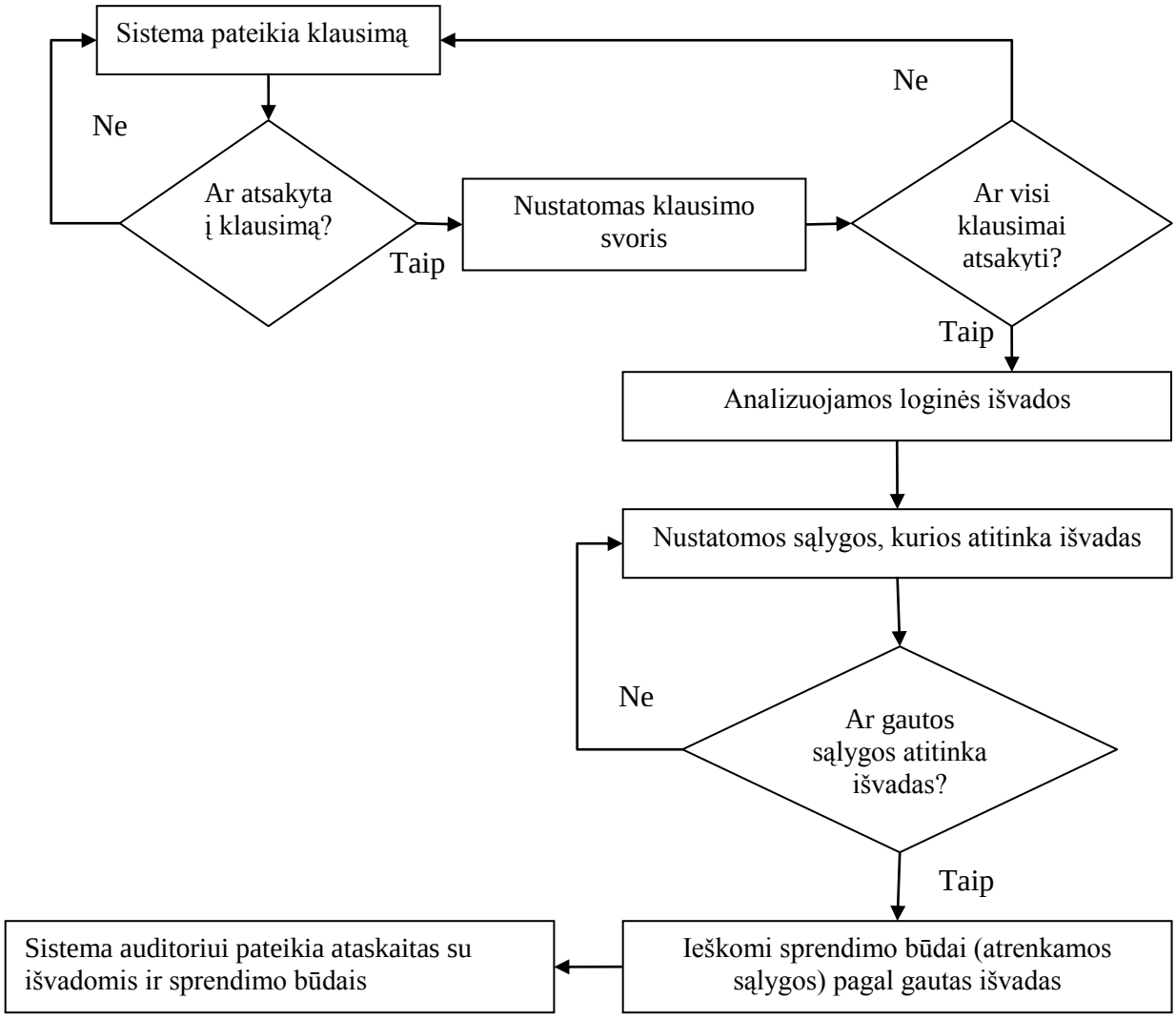
Žinių įvedimo modulis padeda įvesti į kompiuterio atmintį faktus (klausimus) ir taisykles. Žinios, kurias sudaro faktai ir taisyklės, nėra pastovios, jos visą laiką papildomos naujais faktais ir taisyklėmis. Kai kurios iš jų taip pat gali būti panaikintos arba pakeistos. Taigi žinių bazė turi būti nuolat atnaujinama.

Taisyklių žinių bazėje dažniausiai turi deklaratyvią formą, konstatuoja tam tikrus reiškinius. Jie išreiškiami sąlygos sakiniais. Gali būti ir kitų žinių pateikimo būdų, išreiškiamų, pvz., tokiais aplinkybiniais sakiniais, kaip: "jeigu..., tai".

Faktai ir taisyklės, pradiniai duomenys įvedami į kitą modulį, išvadų generatorių. Jis jungia faktus, užrašytus bazėje su atitinkamomis taisyklėmis, užrašytomis taisyklių bazėje. Taip

susidaro nauji faktai, kurie savo ruožtu užrašomi faktų bazėje. Taigi sistema sugeba kurti savo žinių baze.

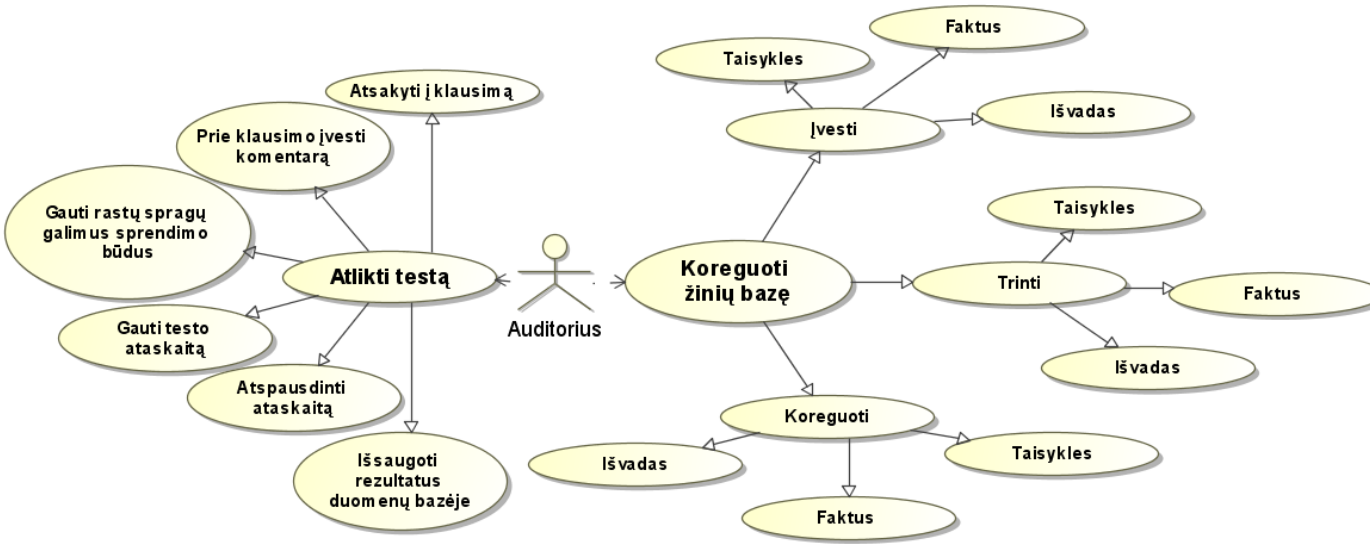
Toliau pateikia asmens duomenų tvarkymo audito išvadų ir esant neatitikimams galimo sprendimo radimo schema. Pirmiausia sistema pateikia klausimą – faktą auditoriui ir tikrina ar šis klausimas yra atsakytas, jei ne, imamas kitas klausimas, o praleistas nukeliamas į pateikiamų klausimų sąrašo pabaigą. Atsakytam klausimui yra nustatomas svoris, tai yra jo svarbumas, aktualumas viso audito metu. Tai turi didelės įtakos generuojant išvadas. Atliekamas tikrinimas ar visi klausimai atsakyti, jei taip pereinama prie loginės išvados analizės. Jei randama, kad atsakyti klausimai neatitinka keliamų reikalavimų, sistema pateikia išvadas, kurios atitinka realią situaciją. Pereinama prie patikrinimo ar gautos sąlygos atitinka išvadas. Viską peržiūrėjus ir gavus patvirtinamą sistema auditoriui pateikia galimas išvadas ir sprendimo būdus, kaip ištaisyti kylančias saugumo problemas.



Pav. 13 Pateikiama sprendimo radimo schema

2.6. Auditoriaus ir sistemos sąsaja

Auditorius naudodamasis asmens duomenų tvarkymo sistemą turės galimybę atlikti du pagrindinius veiksmus, tai yra „atlikti testą“ ir „koreguoti žinių bazę“. Pirmas veiksmas „atlikti testą“ dar skaidomas į smulkesnius veiksmus, tai yra atsakyti į sistemos pateiktą klausimą, įvesti komentarą, gauti testo ataskaitą ir kt. Antrasis veiksmas „koreguoti žinių bazę“ labiau skirtas asmeniui, kuris turi žymiai daugiau patirties šioje srityje. Norėdamas išsamiai įmonėje atlikti asmens duomenų tvarkymo auditą, jis gali papildyti, pakoreguoti, ištrinti (jei yra kokių stiprių pasikeitimų turimuose standartuose) žinių bazėje esančias taisykles, faktus bei išvadas. Žemiau yra pateikiama audituojančio asmens ir asmens duomenų tvarkymo audito sistemos atvaizduojanti schema.



Pav. 14 Auditoriaus ir sistemos bendra sąsaja

2.7. Išvados

1. Projektavimo etape apibrėžti sistemos tikslai, funkciniai ir nefunkciniai asmens duomenų tvarkymo audito sprendimų paramos sistemos reikalavimai.
2. Pateiktas intelektualios sprendimo paramos sistemos ir asmens duomenų tvarkymo audito vertinimo procesas, apibūdinti kiekvieno etapo veiksmai.
3. Pagal ištirtą asmens duomenų tvarkymo audito vertinimo procesą, sumodeliuotas intelektualios sprendimo paramos sistemos (ISPS) vietą jame, taip pat pagal sukurtų ISPS tyrimų rezultatus sumodeliuota kuriamos ISPS struktūra.
4. Pateikta auditoriaus ir sistemos sąsaja. Joje pavaizduota kokius veiksmus galės atlikti auditorius dirbdamas su šia sistema.

3. REALIZACINĖ DALIS

Asmens duomenų tvarkymo audito sistemai kurti naudojama ekspertinė sistema. Kuriant ekspertinės sistemos modulį, naudojami du būdai:

- specialios programavimo kalbos ir aplinkos;
- „tuščios" ekspertinės sistemos, ekspertinių sistemų forma (apvalkalas) – tai iš anksto parengta programa be žinių bazės, taigi ji gali būti pritaikyta bet kokiai dalykinei sričiai (tai priklauso nuo to, kokia žinių bazė bus joje panaudota).

Šiame darbe yra naudojama ekspertinių sistemų forma (apvalkalas).

3.1. Ekspertinės sistemos kūrimo įrankio pasirinkimas

WIN-PROLOG

WIN-Prolog yra galinga AI kalba, kuri numato aukšto lygio ir produktyvią aplinką, kuria remiantis galima daryti logiškas išvadas.

- Palaikomas daugialypis redagavimo langas (pavyzdžiui automatinis sintaksės spalvinimas, daugialypiai šriftai lange, ir t.t.).
- Visapusė teksto paieška.
- WIN-PROLOG leidžia kurti Windows aplinkoje; taip suteikiant patogią prieigą prie Windows Graphical User Interface (GUI) funkcijos. Visos GUI ypatybės, panaudotos aplinkos yra tiesiogiai pasiekiamos Prolog'o programoms.
- WIN-PROLOG atitinka Edinburgo sintaksę suderinama su ISO Prologo standartu.
- WIN-PROLOG grįstas dinamiškos sąsajos bibliotekų (DLL) funkcijomis. DLL parašytas C, C ++, Delphi, Java. Pasinaudodamas WIN-PROLOG duomenų tipų, įvesties ir išvesties funkcijų diapazonu, DLLs gali apsikeisti visų tipų duomenimis su Prolog'o programomis. [28]

e2gLite

e2gLite yra Java programėlė (ang. applet), kuri įterpta į tinklalapį ir parsiunčiama iš internetinio serverio į vartotojo naršyklę. Programėlė įkelia žinių bazę iš serverio ir tada paleidžiama naršyklėje.[29]

Privalumai:

- Žinių bazės failai įkeliami į vartotojo naršyklę, tuo metu ekspertinė sistema gali būti prieinama iš bet kurios interneto ryšį turinčios vietos išskyrus ten, kur draudžiama naudoti server-side Java, Java Server Pages (CGI), Active Server Pages (ASP), Common Gateway Interface (SGI).
- Paprastumas ir lankstumas. Java programėles į tinklalapius perkeliamos taip pat paprastai, kaip ir grafiniai paveikslėliai.
- ekspertinių sistemų forma (apvalkalas) yra nemokama ir gali būti laisvai naudojamas ne komerciniams tikslams.

Trūkumai:

- e2gLite programėlę pirmą kartą siunčiant į naršyklę, naudojantis paprastu modemu, reikia palaukti maždaug 10 sekundžių. Žinių bazės parsisiuntimo laikas priklauso nuo turimo dokumento dydžio. Stengiantis kuo mažiau apkrauti sistemą, patogiausia būtų naudoti iki 100 taisyklių turimas ekspertines sistemas.
- e2gLite žinių bazė yra tekstinis failas perskaitomas naudojantis žiniatinklio serverio Java programėle, dėl šios priežastis kyla grėsmė dokumento konfidencialumui.
- Programėlei veikiant naršyklėje yra naudojama Java virtuali mašina (JVM). Šiuo atveju problemos gali kilti, jei turima naršyklė nepalaiko java technologijos.

Drools Guvnor

Drools Guvnor yra centralizuota Drools žinių bazės saugykla su turtingu interneto GUI redaktoriumi ir priemonėmis skirtomis taisyklių valdymo pagalbai. Drools įrankis leidžia sukurti vykdomąsias žinių bazes. Duomenų saugyklos dalyje laikomos taisyklės, modeliai, funkcijos, procesai ir tt. Prieiga yra kontroliuojama, kad srities ekspertai (ne programuotojai) galėtų peržiūrėti ir redaguoti taisykles be sąlyčio su visomis funkcijomis vienu metu.[30]

- Galimybė kontroliuoti prieigą prie turimų taisyklių ir pan.

- Nebūtinai asmuo turi būti programuotoju, kad sugebėtų grafiniu redaktoriumi redaguoti taisykles.
- Reikia įvaldyti versijas ir taisyklių pakeitimų per tam tikrą laiką.
- Drools srauto procesas yra lengvai įterpiamas į bet kurią "Java" programą (kaip paprastas "Java" komponentas).
- Drools srautas generuoja įvykius per procesų vykdymą, leidžiantį sukurti audito žurnalą, kuriame randama reikalinga informacija, kad išsiaiškinti kas vyksta vykdymo metu. Rezultatai pateikiami XML faile arba saugomi duomenų bazėje.
- ekspertinių sistemų forma (apvalkalas) yra mokama, tačiau yra galimybė nemokamai naudotis ne komerciniams tikslams.

XpertRule

Taisyklėmis pagrįstas ekspertinės sistemos įrankis. Šiame įrankyje sprendimų medžiai yra pagrindinis žinių vaizdavimo metodas. XpertRule automatiškai generuoja sprendimų medį, taip pat naudoja fuzzy argumentus, kuriuos galima integruoti su aiškiais samprotavimais ir GA optimizavimu [31].

- Paprasta taisyklių kūrimo aplinka.
- Integruota sprendimų mašina, žinios pateikiamos naudojantis medžių bei taisyklių kūrimo metodika.
- Pritaikomi žinių objektai.
- Lanksti žinių diegimo parinktis, Ajax technologijos naudojimas, bei COM + XML duomenų mainai.
- Windows ekspertinės sistemos kūrimo įrankis, naudojamas genetiniams algoritmams optimizuoti. Naudojamos C, Pascal ir Cobol programavimo kalbos.
- Palaikoma MS Windows.

JRules

IBM WebSphere ILOG JRules suteikia funkcionalumą kurti ir diegti taisyklėmis grindžiamas taikomąsias programas Java ir SOA pagrindu turinčioje aplinkoje.

- Lengva kurti ir diegti taisyklėmis grindžiamas taikomąsias programas.

- Plačios taisyklių kūrimo galimybės grindžiamos taikomosiomis programomis panaudojant Eclipse IDE (Rule Studio).
- Automatinis taisyklių redagavimas.
- Galimybė lengvai papildyti taisyklių rinkinį.
- Sistemą palaikančios operacinės sistemos: AIX, HP-UX, Linux, Solaris (Sun Microsystems), Windows z / OS
- Ekspertinių sistemų forma (apvalkalas) yra mokama.

Lentelė 4 Ekspertinių sistemų formų (apvalkalų) palyginimas

Ekspertinių sistemų forma (apvalkalas)	Žinių atvaizdavimas ţinių bazėje	Programavimo kalba	Mokama/ Nemokama
WIN-PROLOG	Taisyklių formavimas	C, C ++, Delphi, Java	Nemokama ne komerciniams tikslams
e2gLite	Taisyklių formavimas	Java	Nemokama ne komerciniams tikslams
Drools Guvnor	Taisyklių formavimas	Java	Nemokama ne komerciniams tikslams
XpertRule	Taisyklių formavimas	C ir Cobol	Mokama
JRules	Taisyklių formavimas	Java	Mokama

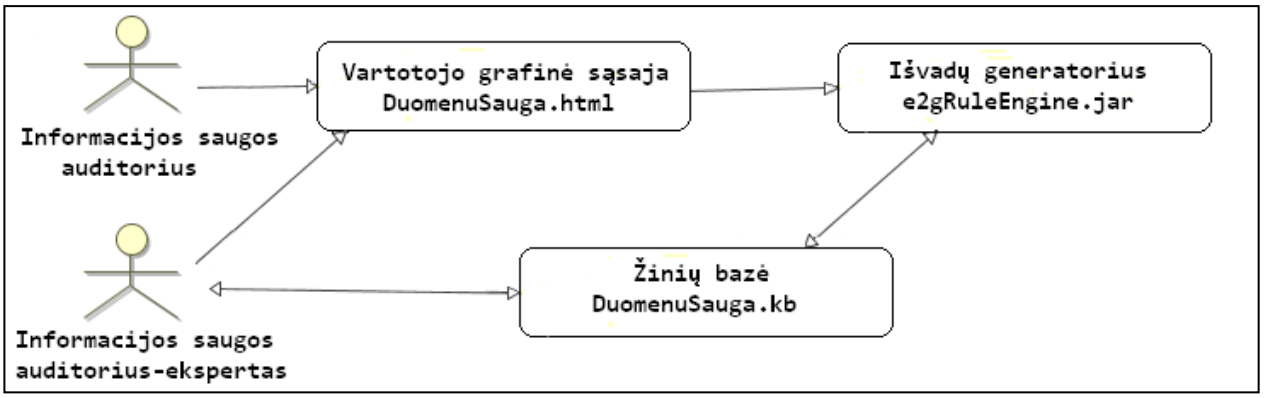
Asmens duomenų tvarkymo audito sistemai kurti buvo pasirinkta **e2gLite** ekspertinės paramos sistema. Ji nesudėtinga bei lanksti. Paprasta grafinė sąsaja. Audito metu nereikalingas sistemos diegimo etapas. Sistema gali būti talpinama pasirinktame serveryje, tokiu būdu pasinaudojus naršyklės programa yra paleidžiama asmens duomenų tvarkymo audito paramos sistema. Šiuo atveju, asmuo norintis atlikti asmens duomenų tvarkymo auditą, galėtų, tai padaryti nevaržomai prie pasirinkto kompiuterio, kuriame būtų interneto ryšys.

3.2. Audito paramos sistemos struktūra

Asmens duomenų tvarkymo sistemos žinių bazė kuriama naudojantis Notepad++ programa. Kūrimo pabaigoje dokumentas išsaugomas „DuomenuSauga.kb“ vardu. Šį dokumentą

sudaro taisyklės, išvados ir klausimynas. Tame pačiame kataloge yra talpinamas išvadų generatorius e2gRuleEngine.jar, o vartotojo grafinė sąsaja perteikiama DuomenuSauga.html turimame dokumente.

Šia sistema gali naudotis informacijos saugos auditorius ir informacijos saugos auditorius-ekspertas. Pirmu atveju, tai gali būti ir įmonės, kurioje norima atlikti auditą esamas darbuotojas atsakingas už asmens duomenų tvarkymo saugumo palaikymą. Antru atveju, asmuo dirbantis šioje srityje, turintis šiokių, tokių žinių bazės kūrimo įgūdžių, bei galintis papildyti turima žinių bazę naujomis taisyklėmis, faktais ir išvadomis.



Pav. 15 Vartotojų ir sistemos sąsaja

3.3. Žinių bazės kūrimo struktūra

Žinių bazės kūrimas susideda iš taisyklių, išvadų ir klausimyno aprašo dalies. Žemiau yra pateiktas žinių bazės kūrimo langas, kuriame matyti taisyklių ir galimų išvadų kūrimo struktūra. Visi šie aprašai saugomi viename dokumente pavadinimu DuomenuSauga su atitinkamu plėtiniu .kb.

Taisyklės aprašomos komanda RULE kartu su galima taisyklės prielaida JEI (IF) ir logine išraiška, kuri susideda iš:

- atributo pavadinimo laužtiniuose skliaustuose;
- naudojamų reliacinių operatorių, tokių kaip lygu (=),mažiau-nei (<) ir daugiau-nei (>), nelygu (!) bei su visomis galimomis išvardintomis reikšmėmis (:);
- lyginamosios reikšmės (true ir false).

Loginiai operatoriai ir (AND)/ arba (OR), jei prielaidos loginių išraiškų yra daugiau, jos yra sujungiamos tuo pačiu loginiu operatoriumi. Kiekvienas prielaidos sakinys susideda iš

atributo pavadinimo, reliacinio operatoriaus, o lyginamoji reikšmė įrašoma kitoje eilutėje. Paskutinis prielaidos sakinys negali baigtis AND arba OR.

Po prielaidos loginės išraiškos rašoma išvada komanda tada (THEN), kuri sudaryta iš:

- atributo pavadinimo laužtiniuose skliaustuose;
- užduoties operatoriaus (=);
- vertės, kuri turi būti priskirta atributui: atitinkamai viengubose arba dvigubose kabutėse, jei tai eilutė. Kitos galimybės yra skaitinės arba loginės TRUE arba FALSE vertės.

Pasirinktinai, jei atributui priskiriama vertė yra su mažesne nei 100% tikimybe, po vertės rašomas simbolis "@" ir skaitinė vertė tarp 1 ir 100, išreiškianti pasitikėjimo faktoriaus dydį.

```
RULE [1.2.1]
IF [saugos dokumentas 1-1] = "Taip" and
[saugos dokumentas 1-2] = "Taip"
Then [Asmens duomenų tvarkymo dokumentas] = "Asmens duomenų tvarkymo dokumentas yra tvarkingas."

RULE [1.2.2]
IF [saugos dokumentas 1-1] : "Taip" "Ne" and
[saugos dokumentas 1-2] : "Taip" "Ne"
Then [Asmens duomenų tvarkymo dokumentas] = "Peržiūrėkite asmens duomenų tvarkymo dokumentą."

REM Asmens duomenų tvarkymas
  RULE [2.1.1]
IF [asmens duomenų tvarkymas 2-1-1]= "Duomenys renkami apibrėžtais ir teisėtais tikslais" and
[asmens duomenų tvarkymas 2-1-1]= "Duomenys tvarkomi tiksliai, sąžiningai ir teisėtai" and
[asmens duomenų tvarkymas 2-1-1]= "Duomenys tikslūs ir, jei reikia dėl asmens duomenų tvarkymo, nuolat atnaujinami" and
[asmens duomenų tvarkymas 2-1-1]= "Netikslūs ar neišsamūs duomenys ištaisomi, papildomi, sunaikinami arba sustabdomas jų tvar
[asmens duomenų tvarkymas 2-1-1]= "Duomenys tapatūs, tinkami ir tik tokios apimties, kuri būtina jiems rinkti ir toliau tvark
[asmens duomenų tvarkymas 2-1-1]= "Duomenys saugomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgia
[asmens duomenų tvarkymas 2-1-2] = "Taip"
Then [Asmens duomenų tvarkymo reikalavimai] = "Tinkamas asmens duomenų tvarkymas. "
```

Pav. 16 Taisyklių aprašo pavyzdys.

Klausimynas aprašomas komanda PROMT su atributo pavadinimu laužtiniuose skliaustuose. Toje pačioje eilutėje yra nurodomas klausimo tipas:

- MultChoice (galimybė pasirinkti vieną iš pateiktų atsakymo variantų),
- YesNo (loginė įvestis su galimomis reikšmėmis „Taip", „Ne", „Aš nežinau")
- ForcedChoice (loginė įvestis su galimybe pasirinkti be „Aš nežinau" alternatyvos),
- Choice (galimybė pasirinkti atsakymą iš išplečiamojo sąrašo),
- AllChoice (priima visus galimus atsakymus į pateiktą klausimą),
- Numeric (priimama vartotojo įrašyta skaitinė vertė).

Pasirinktinai jei pirma PROMPT eilutė baigiama CF tai ekspertinės sistemos naudotojas gali nustatyti pateikto atsakymo pasitikėjimo faktorių. Jei CF yra neapibrėžtas, naudotojo įvestis bus priimta su 100% tikrumu.

Komanda Default gali būti naudojama priskirti į pateikto klausimo atitinkamą atsakymą, jei vartotojas audito atlikimo metu, būtų nenurodęs jokio atsakymo.

Klausimai ir atsakymų variantai yra talpinami kabutėse, kaip pateikta pav. 17.

```
625  PROMPT [asmens duomenų tvarkymas 4-1-1] AllChoice  CF
626  " Kurių duomenų subjekto teisių yra laikasi įmonėje? Pažymėkite teisingus variantus"
627  "Informuoti duomenų subjektą apie asmens duomenų tvarkymą"
628  "Supažindinti duomenų subjektą su asmens duomenimis ir kaip jie yra tvarkomi"
629  "Reikalavimas ištaisyti duomenų subjekto asmens duomenis"
630  "Sunaikinti arba sustabdyti asmens duomenų tvarkymo veiksmus"
631  "Nenaudoti asmens duomenų, jei subjektas nesutinka, kad būtų tvarkomi jo asmeniniai duomenys"
632  "Netinka nei vienas aukščiau pateiktas atsakymas"
633
634  PROMPT [asmens duomenų tvarkymas 4-2-1] ForcedChoice  CF
635  " Ar duomenų valdytojas suteikia duomenų subjektui informaciją apie kuriuos asmens duomenis yra renkama?"
636  "Taip"
637  "Ne"
```

Pav. 17 Klausimyno aprašo pavyzdys

Išvados yra pateikiamos komanda GOAL. Šios komandos gali būti nurodytos prieš arba po klausimyno, bet privalo būti aprašytos po taisyklėmis. GOAL yra atributai, kuriems išvadų generatoriai ieško verčių. Išvadų paieškos procesas baigiasi, kai visos išvados, kurios yra aprašytos (GOAL) komandų dalyje yra išspręstos arba dėl tam tikrų priežasčių, jų išspręsti negalėjo.

```
GOAL [Asmens duomenų tvarkymo reikalavimai]
GOAL [Asmens duomenų saugojimas ir naikinimas]
GOAL [Asmens duomenų teisėto tvarkymo kriterijai]
GOAL [Asmens duomenų teikimas]
GOAL [Asmens kodo naudojimas]
Goal [Asmens duomenų tvarkymas mokslinio tyrimo tikslais]
GOAL [Asmens duomenų tvarkymas statistikos tikslais]
```

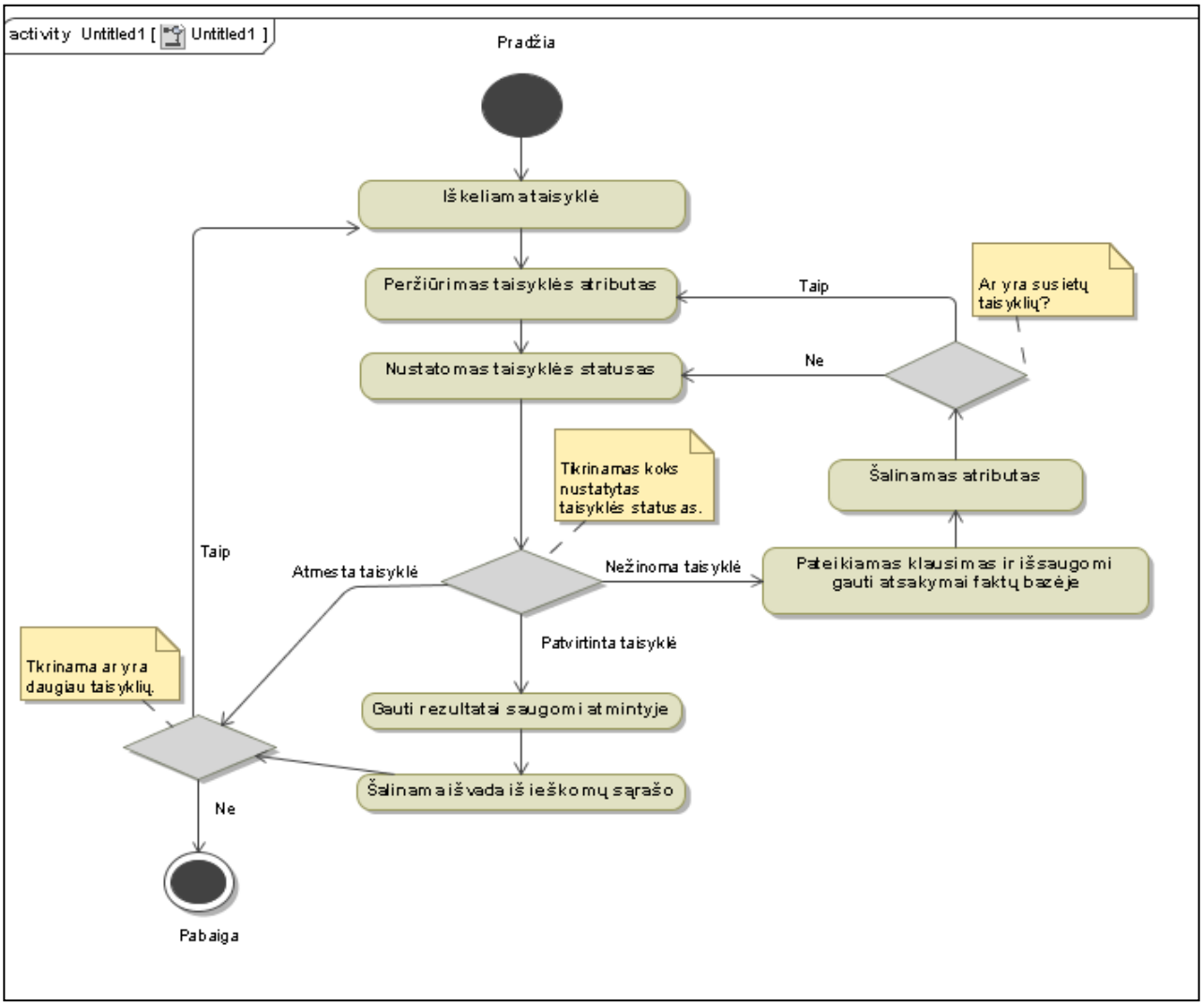
Pav. 18 Išvadų aprašo pavyzdys

3.4. Sistemos dinaminis vaizdas

Remiantis programos išvesties funkcijos langu (Pav. 24), pateikiančiu išvadų generatoriaus veikimą, kuriame sekami visi sistemos atliekami veiksmai audito tyrimo metu. To pasekoje buvo sudaryta sistemos loginė schema, kuri pateikta pav. 19. Iš pateiktos schemos matyti, kad pirmiausiai sistema išsikelia taisyklę, peržiūri tos taisyklės atributą, kadangi pagal jį bus atrenkamas tai taisyklei priskirtas klausimas. Tikrinamas koks turimos taisyklės statusas, tai yra, ar taisyklė „nežinoma“, „patvirtinta“, „atmesta“. Jei taisyklė „nežinoma“, sistema vartotojui pateikia klausimą ir išsaugo gautus rezultatus faktų bazėje. Ištrinamas atributas ir atliekamas tikrinimas ar yra susietų kitų taisyklių. Radus susietas taisykles, sistema peržiūri sekanti atributą ir ciklas vyksta iš naujo, priešingu atveju pereinama prie taisyklės statuso tikrinimo. Šis ciklas trunka tol, kol sistema šį statusą arba „patvirtina“ arba „atmeta“.

Jei sistema nustato, kad taisyklė yra „atmesta“, tuomet peržiūrimos ar daugiau sistemoje yra taisyklių, jei taip, pereina prie kitos taisyklės, jei ne, pateikiamos galutinės išvados.

Sistemai nustačius taisyklės statusą „patvirtinta“, gauti rezultatai yra saugomi atmintyje. Šalinama išvada iš ieškomų išvadų sąrašo ir pereinama prie tikrinimo ar nėra sistemoje daugiau taisyklių. Jei randama kita taisyklė, ciklas kartojasi iš naujo, jei ne, sistema pateikia galutines sprendimo išvadas.



Pav. 19 Sistemos loginė schema

3.5. Sistemos prototipo tyrimas

Sistemos prototipą galimybes padėjo ištirti pasirinktos organizacijos IT specialistas. Gauti rezultatai pateikti 5 ir 6 lentelėje, kurie buvo iškelti sistemos projektavimo metu.

Tyrimo metu buvo peržiūrėti šie sistemos funkciniai reikalavimai:

Lentelė 5 Funkcinių reikalavimų tyrimo rezultatai

Pagal vartotojų pateiktus atsakymus atrinkti tinkamiausius sprendimo būdus iškilusioms asmens duomenų tvarkymo saugumo spragoms spręsti.	*Taip*
Galimybė auditoriui peržiūrėti abejotino klausimo svarbumą.	*Taip*
Visi audito metu gauti duomenys turėtų būti kaupiami ir saugomi.	*Ne*
Galimybė papildyti žinių bazę: kurti taisykles-klausimus, rekomendacijas.	*Taip*

Testavimo metu buvo peržiūrėti šie sistemos nefunkciniai reikalavimai:

Lentelė 6 Nefunkcinių reikalavimų tyrimo rezultatai

Ar nesudėtinga vartotojo sąsaja?	*Taip*
Ar mygtukų paskirtis aiški?	*Taip*
Ar mygtukų išdėstymas nepainus?	*Taip*
Ar lengvai suprantami vartotojui pateikiami klausimai?	*Taip*
Ar klausimai pateikti pagal visus turimus saugumo standartus (LR įstatymai, ES direktyvos ir kt.)?	*Taip*
Ar leidžiama pasirinkti vieną iš dvejų galimų atsakymų?	*Taip*
Ar leidžiama pasirinkti vieną iš kelių galimų atsakymų?	*Taip*
Ar leidžiama pasirinkti kelis galimus atsakymus?	*Taip*
Ar leidžiama nustatyti atsakymo pasitikėjimo faktoriaus reikšmės dydį?	*Taip*
Ar programa reikalauja atsakyti į visus pateiktus klausimus?	*Nereikalauja, jei turima sritis neaktuali įmonei*
Jei nepasirenkamas atsakymas ar jis pažymimas kaip nepasirinktas?	*Taip*
Ar pateikiamos išvados yra suprantamos?	*Taip*
Ar sistema lengvai prieinama?	*Taip*

Kadangi galima prieiga prie sistemos yra naudojantis interneto naršyklėmis, buvo atliktas tyrimas ar jungiantis per pagrindines naršykles neiškils nenumatytų nesklandumų.

Lentelė 7 Sistemos veikimo naudojantis pagrindines naršykles tyrimo rezultatai

Mozilla Firefox	*reikalinga įdiegta Java Plug-in programa, daugiau nesklandumų nerasta.*
Google Chrome	*reikalinga įdiegta Java Plug-in programa, daugiau nesklandumų nerasta.*
Internet Explorer	*reikalinga įdiegta Java Plug-in programa, daugiau nesklandumų nerasta.*
Opera	*reikalinga įdiegta Java Plug-in programa, daugiau nesklandumų nerasta.*

Tyrimo pabaigoje IT specialistas pateikė keletą pastebėjimų, vienas iš jų, tai nėra galimybės gautų rezultatų išsaugoti. Kadangi tuomet būtų galimybė stebėtis po kiekvieno įstaigos patikrinimo ar asmens duomenų tvarkymo saugumo klausimu situacija gėrėja ar blogėja.

Peržiūrėjus į gautus rezultatus galima teigti, kad sistema atitinka beveik visus testavimo metu iškeltus reikalavimus.

3.6. Sistemos prototipo palyginimas su kitais audito įrankiai

Realizuotą sistemą palyginti su kitais audito programiniais įrankiais, skirtais patikrinti įmonėje asmens duomenų saugumą, buvo ganėtinai sunku. Rastos sistemos atliko bendrą informacijos saugos auditą, kurį sudaro ne tik duomenų tvarkymo saugos patikrinimą, bet ir kitas sritis. Sekanti priežastis, rasti įrankiai yra komerciniai, todėl sudėtinga parsisiųsti ir išbandyti visas jo turimas galimybes. Atliekant sistemos prototipo palyginimą su panašiais kitais įrankiais buvo remtasi pateiktais sistemų aprašais, o tyrimo metu iškelti kriterijai buvo atrinkti atsižvelgiant į sukurtos asmens duomenų tvarkymo audito paramos sistemos galimybes.

Lentelė 8 Sistemos prototipo palyginimas su kitais audito programiniais įrankiais

	MKinsight	Cobra	Business Threat modeling methodology PTA (Practical Threat Analysis)	Security Audit Program	Asmens duomenų tvarkymo audito paramos sistema
Asmens duomenų tvarkymo vertinimas	Ne	Ne	Ne	Ne	Taip
Paremta ekspertinių sistemų metodika	Taip	Taip	Taip	Nežinoma	Taip
Galimybė papildyti žinių bazę	Taip	Ne	Taip	Ne	Taip
Suderinamumas su standartais	ISO 27002 (ISO 17799)	ISO 17799	ISO 27001	ISO 27002 (ISO 17799)	LR įstatymai, ISO 17799
Kalbos parinktys	Anglų k.	Anglų k.	Anglų k.	Anglų k.	Lietuvių k.
Pasitikėjimo faktoriaus nustatymas	Ne	Ne	Ne	Taip	Taip
Klausimų paaiškinimų pateikimas	Ne	Ne	Ne	Ne	Taip
Grafinės ataskaitos pateikimas	Taip	Taip	Taip	Taip	Ne
Prieiga prie sistemos	Diegiama programinė įranga	Diegiama programinė įranga	Diegiama programinė įranga	Diegiama programinė įranga	Per interneto naršyklę

3.7. Sistemos funkcinis aprašymas

LR įstaigų asmens duomenų tvarkymo saugumo įvertinimui atlikti, sistema buvo kuriama remiantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, 95/46/E direktyva ir kitais dokumentais reglamentuojančiais saugų duomenų tvarkymą.

Darbo metu buvo iškeltas tikslas sukurti sistemą, kuri palengvintų nustatyti asmens duomenų tvarkymo saugumo lygį turimoje įstaigoje. Tokiu būdu organizacija galėtų greitai reaguoti į iškilusias saugumo spragas ir jas spręsti.

Sistemos kūrimo įrankis buvo pasirinktas atsižvelgiant į galutinį vartotoją, kuris neturėdamas stiprių programos kūrimo įgūdžių galėtų patobulinti turimą sistemą papildydamas žinių bazę.

3.8. Sistemos instaliavimo vadovas

Asmens duomenų tvarkymo audito paramos sistemai reikalinga naršyklė. Naršyklės pasirinkimas (Internet Explorer, Mozilla Firefox, Google Chrome) ir versija neturi įtakos sistemos veikimui, tačiau sistemos paleidimo pradžioje gali išvesti užklausa dėl ActiveX valdiklių, kartais vadinamu priedais leidimo diegti. Jie būtini sistemos veikimo palaikymui.

Sekantis svarbus įrankis palaikyti tinkamą sistemos veikimą yra Java Plug-in programa.

Audito paramos sistemą gali būti talpinama serveryje, taip auditoriui supaprastinant prieigą prie turimos sistemos. Serveryje, kuriame nėra draudžiama naudotis Java Server Pages (CGI), Active Server Pages (ASP), Common Gateway Interface (SGI).

Sistemos paleidimas iš savo kompiuterio. Iš turimo katalogo yra paleidžiamas DuomenuSauga.html dokumentas.

3.9. Sistemos administracinis vadovas

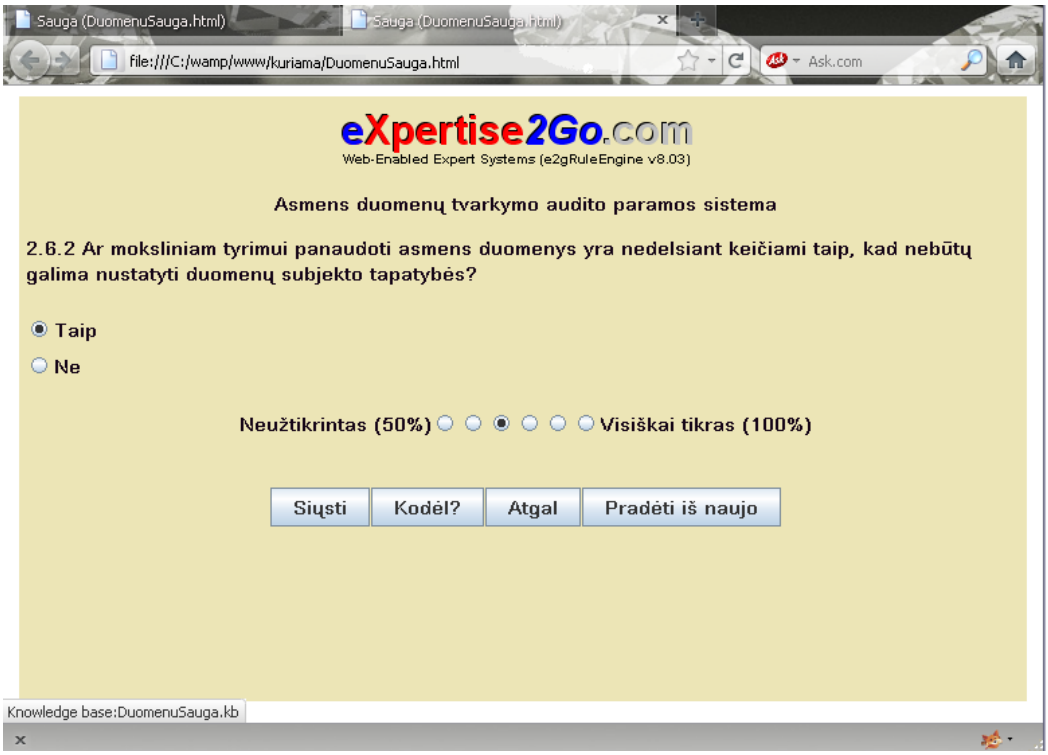
Sistemos administracinis vadovas turi galimybę papildyti turimą žinių bazę naujomis taisyklėmis ir faktais. Šiems papildymams atlikti reikia turėti bent minimalių e2gLite programos naudojimosi įgūdžių.

3.10. Sistemos vadovas

Programinis įrankis skirtas įmonėje atlikti Asmens duomenų tvarkymo saugumo analizę, remiantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, 95/46/E direktyva ir kitais dokumentais reglamentuojančiais saugų duomenų tvarkymą.

3.10.1 Vartotojo grafinė sąsaja

Grafinė vartotojo sąsaja pateikiama pasirinktos naršyklės lange.

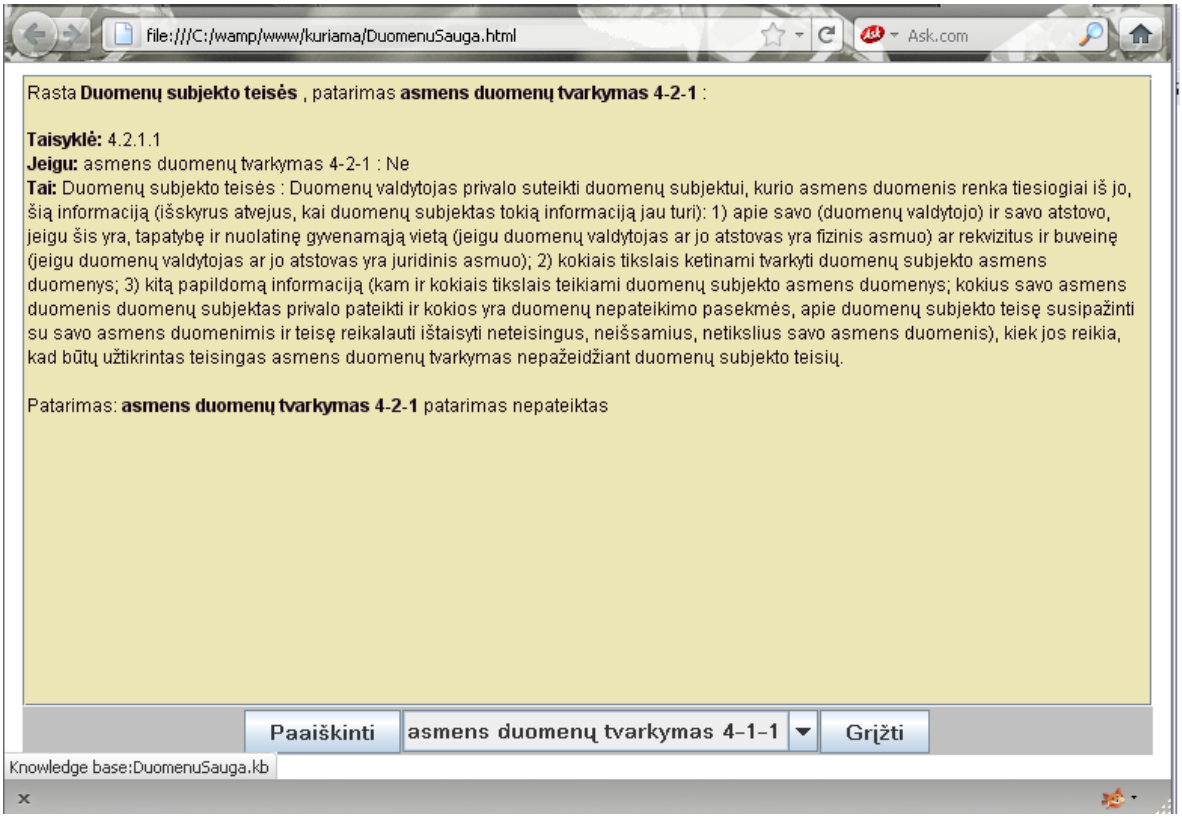


Pav. 20 Grafinės vartotojo sąsajos pateikimas Mozilla Firefox naršyklėje

Asmens duomenų tvarkymo audito paramos sistemos valdymas nėra sudėtingas. Sistemos meniu dalį sudaro šie pagrindiniai mygtukai:

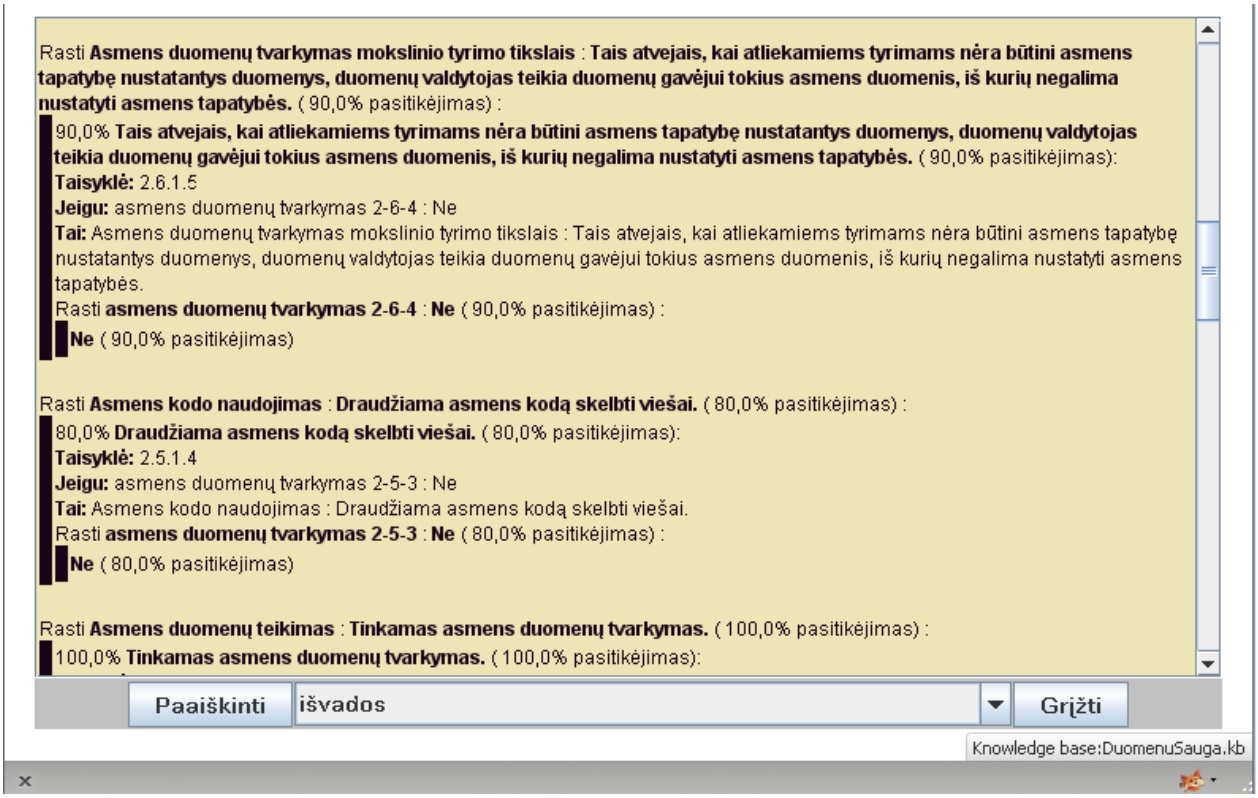
- *„Siųsti“* – į išvadų generatorių siunčiami pažymėtų atsakytų variantai;
- *„Kodėl“* pateikia išsamų aprašymą kodėl šis klausimas yra aktualus, remiantis taisyklėmis ir faktais.
- *„Atgal“* - galimybė grįžti prie klausimo ir peržiūrėti pateiktus rezultatus, bei siūlomas rekomendacijas.
- *„Grįžti“* – pereiti į prieš tai atidarytą programos langą.
- *„Pradėti iš naujo“* – galimybė grįžti prie klausimyno pradžios ir testą pradėti iš naujo.
- *„Išvados“* – galimybė peržiūrėti norimos srities testų rezultatus. Pasirinkus sritį, reikia paspausti mygtuką *„Paaiškinti“*.

Iškilus neaiškumui dėl turimo klausimo būtinumo sistema pateikia šio klausimo svarbumą remiantis taisyklėmis ir faktais. Ši funkcija iškviečiama mygtuku *„Kodėl“*.



Pav. 21 Sistemos vartotojui pateikiamas klausimo svarbumas

Apačioje pateiktas langas, kuriame galima peržiūrėti vartotojo pasirinktas reikšmes, atsakymus, bei jiems priskirtas reikšmes. Pateikiami skaičiavimai išvadoms gauti.



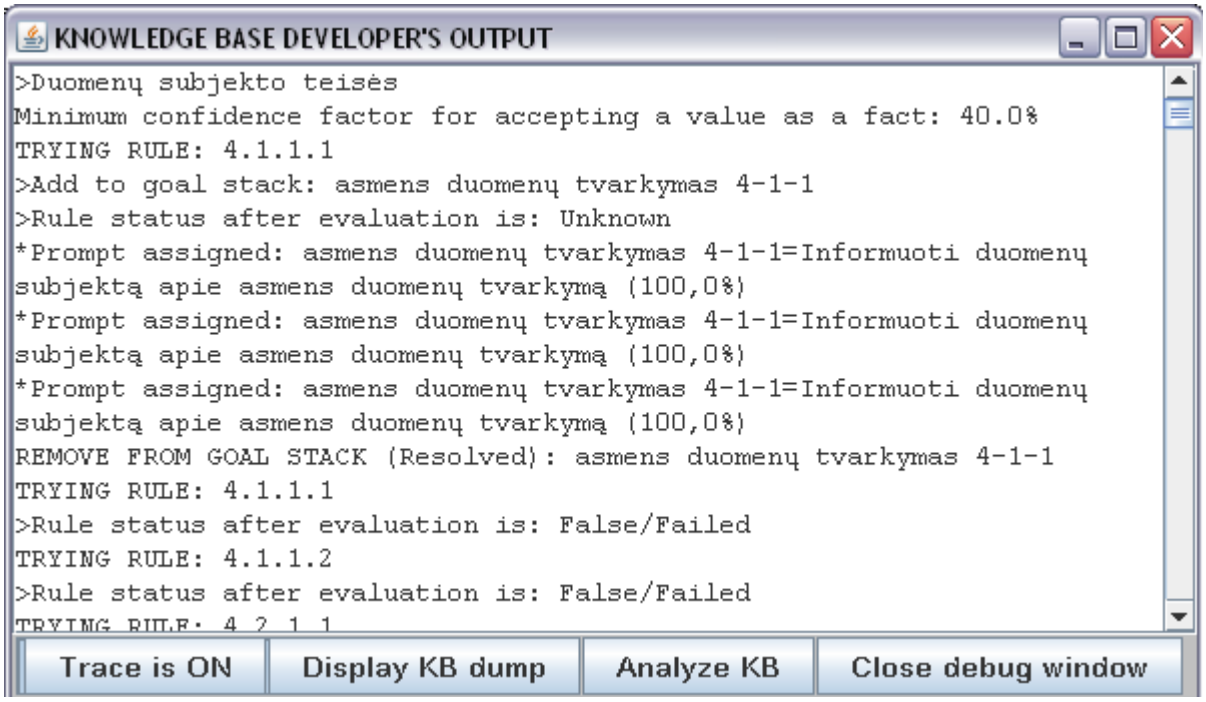
Pav. 22 Grafinė vartotojo sąsaja, išvadų pateikimas

Pav. 22 pateikiami įmonėje atlikto audito gauti daliniai rezultatai. Sistema audito metu ras 2006/123/EBndus saugumo spragas, jas pateikia šiame lange su galimomis rekomendacijomis.

Sistemos vartotojas (auditorius) gali peržiūrėti savo pateiktus atsakymus. Kaip matome iš pav. 22 į asmens kodo naudojimo pateiktus klausimus auditorius pateikė ir neigiamų atsakymų, todėl sistema primena, kad būtų aptarta su asmens duomenimis dirbančiu darbuotojų personalu dėl asmens kodo viešinimo, bei atsakomybę už šio nuostato nesilaikymo.

3.10.2 Žinių bazės programos išvesties funkcija

Papildoma informacija apie audito vykdymą galima peržiūrėti išvesties funkcijos lange, kuris pateiktas pav. 23 pavyzdyje. Ši funkcija iškviečiama pažymėjus sekimo mygtuką „Trace is on“



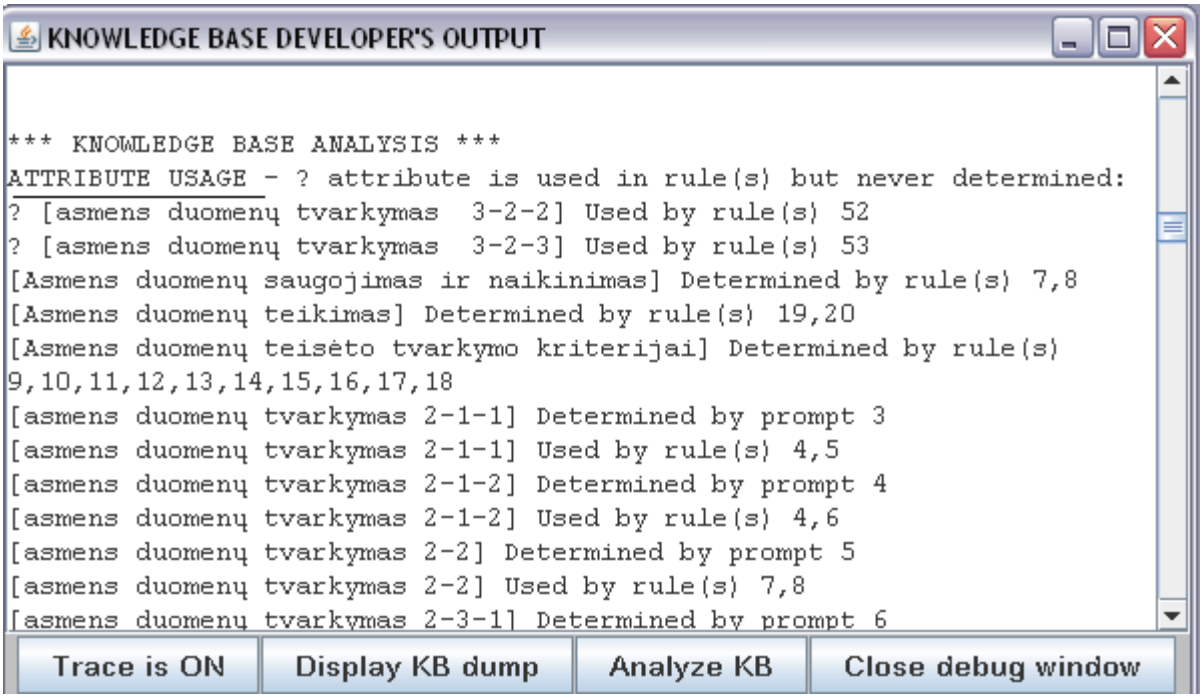
Pav. 23 Žinių bazės programos išvesties funkcija

Atsidarius programos išvesties funkcijos langui, e2gRuleEngine išvadų generatorius veikia sekimo režimu, kuriame vienas po kito rodomi atliekami sistemos veiksmai, tai yra pateikiama minimali audito metu galima pasitikėjimo faktoriaus reikšmė.

Papildomos žinių bazės programos išvesties funkcijos:

- Trace is ON / OFF – įjungiamas arba išjungiamas audito metu atliekamas sekimo režimas.
- Display KB dump –
- Analyze KB –
- Close debug window – mygtukas langą uždaro. Jį dar kartą atidaryti galima tik perkrovus internetinį puslapį, kad e2gRuleEngine išvadų generatorius pasileistų iš naujo.

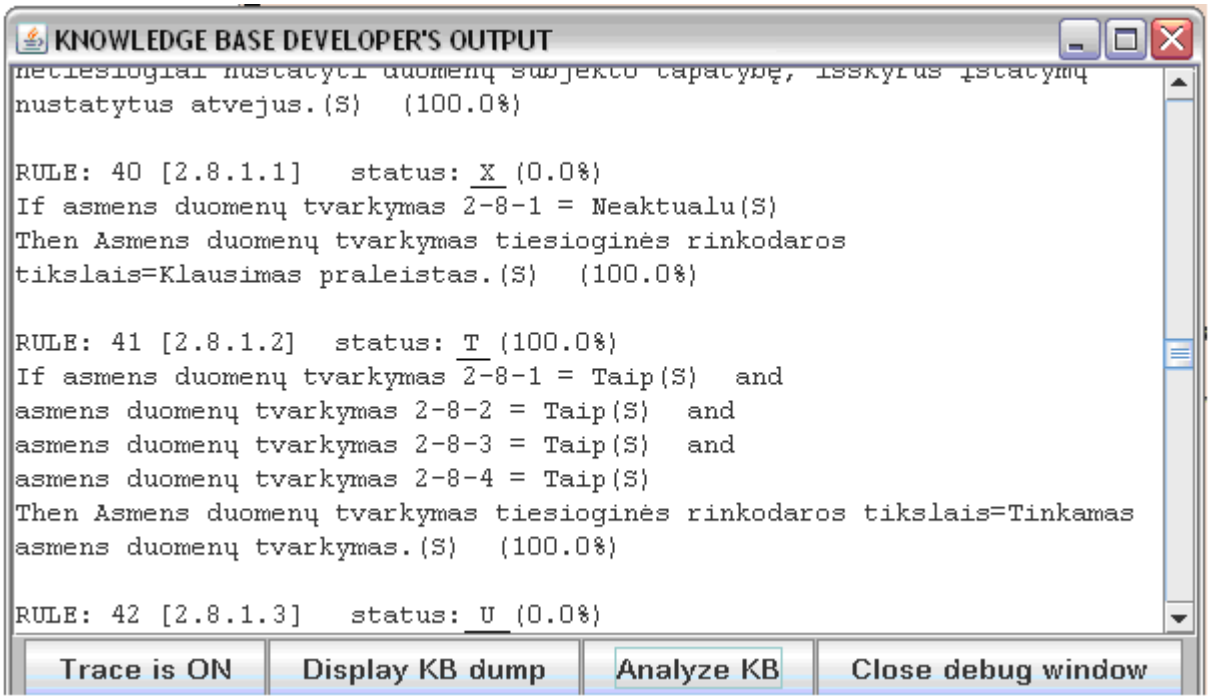
Žinių bazės analizė yra naudinga ieškant spausdinimo ar loginių klaidų žinių bazėje, kurių nesimato kai žinių bazė yra pakrauta. Dažnai pasitaiko spausdinimo klaidų atributų pavadinimuose ir vertėse.



Pav. 24 Išvesties funkcijos langas

Šios išvesties funkcijos požymių aprašymo dalyje (ATTRIBUTE USAGE) visi žinių bazėje rasti atributų pavadinimai yra išvardyti abėcėlės tvarka. Iš pradžių rodomas kiekvienas žinių bazės komponentas (PROMT ir RULE), kuris gali nustatyti atributo vertę. Tada pateikiama kiekviena taisyklė (RULE) naudojanti atributą. Atributas, kuris yra naudojamas, bet nėra nustatytas, reiškia loginę klaidą ir prieš tokio atributo pavadinimą atsiranda klaustukas. Dažniausiai tai atsitinka, nes atributo pavadinime randama klaidų, tokių kaip du vienodi atributai, kai numatytas yra tik vienas.

Išvadų aprašymo dalyje (VALUE USAGE), žinių bazėje randamos tekstinės vertės yra išvardytos abėcėlės tvarka. Kiekviena vertė yra skliaustuose. Kartu su susijusiu atributu, nustatoma jos vieta žinių bazėje (taisyklės prielaidoje, visoje taisyklėje arba PROMPT). Vėlgi, ši išeities funkcija turėtų padėti rasti vertes, kurios parašytos šiek tiek kitaip, tai gali būti daugiau tarpų komandų aprašų arba kiti skyrybos ženklai, todėl dėl šių priežasčių atsiranda dvi vertės, kurios turėtų atitikti, bet neatitinka išvadų generatoriaus reikalavimų.



Pav. 25 Išvesties funkcijos langas

Vienintelis atributas su žinoma verte yra dalyvavimas (ang. precipitation) ir jo vertė (numatomą) vertę parodoma iškelties duomeniu.

Duomenų tipas (S-eilutė, N-skaitinis, B-loginis) rodomas skliaustuose po esama verte. Toliau pateikiamas atributo vertės tikrumo faktorius (100%) skliausteliuose: 0% tikrumas reiškia, kad vertė vis dar nenustatyta. Jei numatytoji (ang, DEFAULT) vertė galima atributui, jo vertei ir tikrumui, kuriam ji bus priskirta, ji bus rodoma paskutinė.

Kiekviena taisyklė rodoma kartu su jos aprašymu ir būsena. U reiškia, kad taisyklės būsena nežinoma ir kad iki šiol abiejų taisyklių žinių bazėje vertės nežinomos. T žymima, jei taisyklė įrodyta kaip teisinga (ang. TRUE) ir todėl buvo paleista, F – jei taisyklė įrodyta kaip klaidinga (ang. FALSE) ir X – jei išvadų generatorius nustatė, kad taisyklės neįmanoma įrodyti nei kaip teisinga (ang. TRUE), nei kaip klaidinga (ang. FALSE). Taisyklės tikrumo faktorius nurodomas eilutės pabaigoje. Kiekvienos vertės, naudojamos prielaidoje arba toliau taisyklėje, duomenų tipas (S-eilutė, N-skaitinis, B-loginis) rodomas skliausteliuose po vertės. Tikrumas, kuriam bus priskirta tolesnė vertė, rodomas skliausteliuose kiekvienos sekančios eilutės pabaigoje

3.11. Išvados

1. Pasirinktas įrankis, kuriuo naudojantis buvo kuriama asmens duomenų tvarkymo audito paramos sistema. Renkantis įrankį buvo iškelti šie kriterijai, tai yra, nemokama sistema, nesudėtinga vartotojui grafinė sąsaja, galimybė auditoriui papildyti turimą žinių bazę.
2. Naudojantis e2glite ekspertinės sistemos apvalkalu buvo sukurta asmens duomenų tvarkymo audito paramos sistema.
3. Sukurta sistema pritaikyta naudotis dvejiems sistemos vartotojams, tai yra paprastam auditoriui ir auditoriui ekspertui, pastarasis, turės galimybę papildyti turimą žinių bazę.
4. Sistema sukurta remiantis LR teisiniai aktais, ES direktyvomis bei ISO/IEC 17799 ir LST ISO/IEC 27001 standartais, kuriuose kalbama apie asmens duomenų tvarkymą.
5. Sukurta sistema buvo palyginta su kitomis auditui skirtomis sistemomis, be to, pasirinktoje įmonėje atliktas šio įrankio įvertinimas.

4. IŠVADOS

1. Apžvelgta asmens duomenų sąvoka bei su jos tvarkymu susijusios kylančios problemos. Peržiūrėti LR teisiniai aktai, ES direktyvos bei ISO/IEC 17799 ir LST ISO/IEC 27001, kuriuose kalbama apie naudojamų asmens duomenų saugumą, darbuotojų patikrinimą, tai yra ar neviešina turimos informacijos, ar nenaudoja saviems piktavališkiems tikslams ir kt.
2. Peržiūrėta ar yra atitinkamų įrankių, skirtų įmonėje patikrinti ar tinkamai tvarkomi asmens duomenys.
3. Darbo metu buvo iškeltas tikslas sukurti asmens duomenų tvarkymo audito paramos sistemą, kuri palengvintų priimti sprendimus ir pateiktų rekomendacijas duomenų tvarkymo saugumo palaikymo. Sistema sukurta remiantis visais teisiniais standartais, kuriuose minimas apie asmens duomenų tvarkymo saugumą.
4. Pagal ištirtą asmens duomenų tvarkymo audito vertinimo procesą, sumodeliuotas intelektualios sprendimo paramos sistemos (ISPS) vietą jame, taip pat pagal sukurtų ISPS tyrimų rezultatus sumodeliuota kuriamos ISPS struktūra.
5. Teigiant, kad magistrinio darbo tikslas pasiektas, galima paminėti išvadas:
    a. Naudojantis ekspertinės sistemos apvalkalu buvo sukurta asmens duomenų tvarkymo audito paramos sistema, kuri yra paremta LR teisiniais aktais ir ISO 27001 standartu.
    b. Sistema pritaikyta paprastam vartotojui ir auditoriui ekspertui, kuris turės galimybę koreguoti ar papildyti turimą sistemą.
    c. Atlikus auditui skirtų įrankių analizę, pastebėta, kad rastos sistemos yra daugiau skirtos plačiai įmonėje vykstančiai veiklai, o be to, dauguma jų yra komercinės, todėl negalima pilnai ištyrinėti jų visas galimybes.
    d. Ištyrus rastus įrankius, pastebėta, kad dauguma jų yra diegiamos į kompiuterį, o šiuo atveju sukurta sistema turi privalumą, kad galima prieiga per interneto naršyklę.
    e. Įvertinus prototipo sistemos kokybę, galima teigti, kad sistemos sąsaja yra patogi, aiški vartotojui, yra galimybė ją koreguoti, papildyti.
    f. Sistemos pastebėjimai, trūkumai: nėra galimybės išsaugoti gautų rezultatų.

5. LITERATŪRA

1. [interaktyvus]. [žiūrėta 2009-11-19], prieiga per internetą http://ec.europa.eu/youreurope/nav/en/citizens/services/eu-guide/data-protection/index_lt.html
2. „Lietuvos respublikos asmens duomenų teisinės apsaugos įstatymas. Vilnius. 2008,. [interaktyvus]. [žiūrėta 2009-11-19], prieiga per internetą http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=314801
3. Yohko Orito and Kiyoshi Murata. rethinking the concept of information privacy: a japanese perspective.
4. Ina Wagner. Ethical issues of healthcare in the information society. 1999. http://ec.europa.eu/european_group_ethics/docs/avis13_en.pdf
5. M. Civilka. Asmens duomenų apsauga tarptautinėje ir EB teisėje. Vilnius. 2001,
6. Europos Bendrijų konvencija. 1995, [interaktyvus]. [žiūrėta 2009-12-15], prieiga per internetą. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:19:08:41995A1127(02):LT:PDF
7. ADA Direktyvos 95/46/EB 29 str., [interaktyvus]. [žiūrėta 2009-12-15], prieiga per internetą http://www.ada.lt/index.php?lng=lt&action=page&id=167
8. Europos komisija. Asmens duomenų apsauga Europos sąjungoje. 2008, [interaktyvus]. [žiūrėta 2009-12-15], prieiga per internetą. http://ec.europa.eu/justice_home/key_issues/data_protection/data_protection_0108_lt.pdf
9. Peter Blume. The Citizens Data Protection, [interaktyvus]. [žiūrėta 2009-12-15], prieiga per internetą http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1998_1/blume/
10. „Lietuvos respublikos asmens duomenų teisinės apsaugos įstatymas. Vilnius. 2009, [interaktyvus]. [žiūrėta 2009-12-15], prieiga per internetą. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=314940
11. Aplinkos vadybos auditas, [interaktyvus]. [žiūrėta 2009-12-15], prieiga per internetą http://aplinkotyra.vdu.lt/uploads/file/moduliai/aplinkosaugos_vadyba/aplinkosaugos_vadyba_Paskaitu_medziaga/pAplinkos_vadybos_auditas.pdf
12. Prof. Dr. Wolfgang Kilian . Mokymo apie asmens duomenų apsaugą konvencija. Hanoverio universitetas, [interaktyvus]. [žiūrėta 2009-12-15], prieiga per internetą. www.itc.tf.vu.lt/mokslas/adak.doc

13. Europos sąjungos norminiai teisės aktai, [interaktyvus]. [žiūrėta 2009-12-16], prieiga per internetą. http://eur-lex.europa.eu/lt/dossier/dossier_02.htm
14. E. Kazanavičius, A. Venčkauskas ir kt. Informacijos saugos vadyba. Kaunas, 2008
15. Implementation of Security Policies Based on the BS7799 / ISO 17799 Standard, [interaktyvus]. [žiūrėta 2009-12-16], prieiga per internetą http://www.infoedge.com/samples/CA-0001free.pdf
16. [interaktyvus]. [žiūrėta 2009-12-16], prieiga per internetą http://17799.denialinfo.com/securitypolicies.htm
17. [interaktyvus]. [žiūrėta 2009-12-16], prieiga per internetą http://www.vivaceproject.com/content/advanced/49Kamel.pdf
18. D. Dzemydienė. Intelektualizuotų informacinių sistemų projektavimas ir taikymas. Vilnius. 2006
19. A. Kaklauskas, E. K. Zavadskas. Internetinė sprendimų parama. Vilnius. 2002,
20. J. Adomaitis. Verslo sprendimų paramos sistemų klasifikacija ir tipai. Vilnius: VU leidykla.
21. E. Merkevičius, G. Garšva, O. Cepkovataja. intelektualios sprendimų paramos sistemos struktūra kredito rizikos vertinimui. Kaunas. Psl. 725
22. Stasys Matelis. Intelektualios informacijos apsauga įmonėse, [interaktyvus]. [žiūrėta 2010-03-03], prieiga per internetą http://www.esecurity.lt/article/1322.html
23. Valstybinė duomenų apsaugos inspekcija. Svarbu žinoti vadovui. 2005, [interaktyvus]. [žiūrėta 2010-03-03], prieiga per internetą http://ada.lt/index.php?lng=lt&action=page&id=90
24. E. Kazanavičius, A. Liutkevičius, A. Vrubliauskas. Informacijos saugos vadyba. II dalis. KTU, 2008
25. Vidaus audito rekomendacijos, 2003
26. A.Hamilton. IT62 Decision Support Systems. Lectures. University of Stirling 2004.
27. G. Kulvietis, R. Kulvietienė, V. Rudzkienė. Įvadas į dirbtinio intelekto ir ekspertinių sistemų kursą, Vilnius „Technika“, 1996
28. Rebecca Shalfield, Win-Prolog user guide, London, 2002
29. e2gLite Expert System Shell, [interaktyvus]. [žiūrėta 2010-11-19], prieiga per internetą, http://www.expertise2go.com/webesie/e2gdoc/e2gmod1.htm

30. Centralised Knowledge Repository, [interaktyvus]. [žiūrėta 2010-11-19], prieiga per internetą http://www.jboss.org/drools/drools-guvnor.html
31. [interaktyvus]. [žiūrėta 2010-11-19], prieiga per internetą http://www.xpertrule.com/pages/products.htm
32. Building and Using Expert Systems: a Mini-Course Introducing the e2gRuleEngine/e2gDroid Expert System Shell and e2gRuleWriter Decision Table Software, [interaktyvus]. [žiūrėta 2010-11-19], prieiga per internetą http://www.expertise2go.com/e2g3g/e2g3gdoc/e2gmod4.htm
33. PTA (Practical Threat Analysis) Professional risk assessment software, [interaktyvus]. [žiūrėta 2011-05-02], prieiga per internetą, http://www.software.co.il/downloads/BusinessThreatModeling_4.0.pdf
34. Security Audit Program, [interaktyvus]. [žiūrėta 2011-05-02], prieiga per internetą, http://www.itgovernanceusa.com/product/1643.aspx

Support system for Personal data processing audit development and research summary

Summary

The aim of the paper is to create personal data management's decision support system, which would help auditors to find faster and more accurate decision to personal data management's security problems that may arise in the company. During the research the analysis has been made; similar tools for personal data management's audit have been searched; legal documents, related to personal data management, such as orders of Republic of Lithuania, EU directives and other, have been reviewed.

The system is created using a decision support systems development methodology. According to this methodology, the system selects or helps to select in a certain view the best or at least acceptable alternative from alternative sets, which have been formed by the system or given to it.

The created system is not only used to audit the company in accordance with established security requirements, but also it gives an opportunity to complement or correct existing personal data management's audit support system.