KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Giedrė Jankauskienė

Informacijos saugos audito sprendimų paramos sistema

Magistro darbas

Darbo vadovas
doc. A. Venčkauskas

Kaunas, 2010

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Giedrė Jankauskienė

Informacijos saugos audito sprendimų paramos sistema

Magistro darbas

Recenzentas
prof. dr. R. Butleris
2010-05-26

Vadovas
doc. A. Venčkauskas
2010-05-26

Atliko
IFN-8/3 gr. stud.
Giedrė Jankauskienė
2010-05-26

Kaunas, 2010

TURINYS

DECISION SUPPORT SYSTEM FOR INFORMATION SECURITY AUDIT

SUMMARY

The purpose of this work is to create the information system for information security audit that help to make the decision-making easier for information security auditors and make accurate recommendations to improve safety. The system helps determine the risk factors according to LST ISO/IEC 27001:2006 standard.

The information security audit is high cost and complex process, therefore rarely or not at all performed in organizations. Consequently, there is a need of measures to perform audit by lay persons. Also require that such measures are long term and could be extended, changed, according to political and technological changes in organization.

In this work has been analyzed possibilities and use of decision support systems for information security audit problems solving, developed information security audit decision support system model and realized and tested a prototype system.

Lentelių sąrašas

Paveikslėlių sąrašas

ĮVADAS

Informacijos saugos auditas yra organizacijos politikos, procedūrų, standartų, priemonių ir praktikų, apsaugančių elektroninę informaciją nuo praradimo, sugadinimo, netyčinio atskleidimo, vertinimas [30].

Profesionalios audito organizacijos pabrėžia būtinybę rūpintis informacijos sauga, dėti visas pastangas jai užtikrinti ir teikia rekomendacijas IS saugumo auditui.

Auditoriaus darbo procesas yra sudėtingas ir atsakingas, nuolatos dokumentuojamas ir pakartotinai atliekamas. Todėl detali gaunamų duomenų analizė ir technika, kuria naudojantis ji yra atliekama, yra raktas sėkmingam auditui atlikti. Saugos audito procedūra turi įvertinti bendrovės pagrindinius apsaugos ir kontrolės standartus, apibrėžti kolektyvinio saugumo politiką.

Dėl sudėtingo proceso bei didelių kaštų vidinis informacijos saugos auditas daugumoje organizacijų yra atliekamas retai arba visai neatliekamas. Todėl reikalingos priemonės, kad auditą galėtų nesudėtingai atlikti neprofesionalas informacijos saugos auditorius, t.y. organizacijos darbuotojas, atsakingas už informacijos saugą, bei visam vadovaujančiam personalui, neturinčiam specifinių techninių saugos arba auditavimo žinių, bet galintiems prieiti prie svarbios informacijos. Taip pat reikia, kad tokios priemonės, būtų ilgalaikės bei galėtų būti plečiamos, keičiamos, atsižvelgiant į organizacijos politinius bei technologinius pasikeitimus.

Šio darbo metu buvo išanalizuota informacijos saugos audito svarba ir padėtis Lietuvoje, atlikta pasaulinėje rinkoje esamų priemonių, skirtų IS auditui analizė, išanalizuotos sprendimų paramos sistemų galimybės ir pritaikymas IS audito problemai spręsti, realizuotas ir ištirtas sistemos prototipas.

1. INFORMACIJOS SAUGOS AUDITO METODŲ IR PRIEMONIŲ ANALIZĖ

1.1. Informacijos saugos audito problema

Auditas yra atskirų organizacijos funkcionavimo sričių nepriklausoma ekspertizė [33]. Auditas nagrinėja ne tik išteklių apskaitą, bet ir tai, kaip jie yra panaudojami ir kiek jie yra kritiniai sėkmingam kiekvienos užduoties užbaigimui.

Informacijos auditas reikalingas [33]:

- nustatyti rizikoms, susijusioms su galimomis informacijos saugos resursų grėsmėmis;
- esamo informacijos saugos lygio įvertinimui;
- informacijos saugos silpnų vietų lokalizavimui;
- informacijos saugos atitikimo standartams įvertinimui;
- naujų saugos mechanizmų diegimo ir esamų informacinės saugos mechanizmų efektyvumo didinimo rekomendacijų ruošimui.

Informacijos audito procesas gali paskirstyti informacijos srautus organizacijos viduje, bei tarp organizacijos ir jos išorinės aplinkos. Informacijos auditas nustato esamus kanalus, kuriais galima vykdyti žinių perdavimą [16].

Audito sėkmė priklauso nuo rizikos analizėje dalyvaujančių darbuotojų kompetencijos, patirties, informacijos ir duomenų saugos užtikrinimo metodų. Sėkmingam rizikos analizės procesui reikia, kad saugos politika bei veiksmai atitiktų pačios įstaigos uždavinius, taip pat būtina vadovybės parama.

"Ekskomisarų biuras" atlikto tyrimo duomenimis daugumoje įmonių nėra tinkamos informacinių sistemų ir konfidencialios informacijos apsaugos sistemos, ir net 64% įmonės nepagrįstai mano, kad jų kompiuterinės sistemos yra saugios. Juo labiau, kad mažiau nei 50% apklaustųjų naudoja tinklo apsaugos priemones bei šifravimą. Ir tik 22% apklaustųjų nurodė, jok yra šifruojama slapta informacija [20].

Nors įstatymais apibrėžta sauga Lietuvos valstybinėse institucijose, tačiau realybėje tai retai kada yra atliekama. Tam neskiriama lėšų ir teigiama, kad nėra operuojama su aukštos svarbos duomenimis, taip nuvertinant turimą informacinę bazę.

Pagrindinis darbo tikslas – informacijos saugos audito paramos sistema, kuri palengvintų priimti sprendimus ir pateiktų rekomendacijas informacijos saugai sustiprinti. Sistema padės nustatyti rizikos faktorius pagal LST ISO/IEC 27001:2006 standarto reikalavimus.

Magistrinio darbo tikslo įgyvendinimui buvo iškelti uždaviniai:

1. Išanalizuoti informacijos saugos audito svarbą ir padėtį Lietuvoje;
2. Atlikti pasaulinėje rinkoje esamų priemonių, skirtų IS auditui analizę;
3. Išanalizuoti sprendimų paramos sistemų galimybes ir pritaikymą IS audito problemai spręsti;
4. Sukurti IS audito sprendimų paramos sistemos modelį;
5. Realizuoti ir ištirti sistemos prototipą.

1.2. Informacijos saugos standartai ir teisiniai dokumentai

Lietuvos Respublikos Vyriausybė, siekdama užtikrinti duomenų saugos konfidencialumą ar net siekdama apsaugoti nuo duomenų sunaikinimo, 1997 m. rugsėjo 4 d. nutarimu Nr. 952 patvirtino bendruosius duomenų saugos reikalavimus bei nuostatas [28]. Jų tikslas – sudaryti sąlygas saugiai automatizuotu būdu tvarkyti duomenis. Įstaigų registrams ir kitoms informacinėms sistemoms jie yra privalomi, savivaldybėms - rekomendacinio pobūdžio. Šie reikalavimai taip pat yra taikytini informacinėms sistemoms, kuriose yra apdorojamos tarnybos paslaptys.

Taip pat 2001 m. gruodžio 22 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 1625 buvo priimtas įstatymas „dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ [22], kuriame pateikiama informacijos saugos vertinimo tvarka ir kriterijai.

Užtikrinant informacijos saugą, rekomenduojama vadovautis Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo metodai“ grupės standartais, apibūdinančiais saugų informacinės sistemos duomenų tvarkymą. Visi šiuo metu Lietuvoje pripažinti informacinių technologijų srities informacijos saugos standartai pateikti nr. 1 lentelėje [24].

1 lentelė. Lietuvoje pripažinti naudojami ISO su informacijos sauga susiję standartai

Standartas	Aprašymas
LST ISO/IEC 17799:2005	Informacijos saugumo valdymo praktikos kodeksas (tapatus ISO/IEC 17799:2005)
LST ISO/IEC 27001:2006	Informacijos saugumo valdymo sistemos. Reikalavimai (tapatus ISO/IEC 27001:2005)
LST ISO/IEC 27002:2009	Informacijos saugumo valdymo praktikos kodeksas (tapatus ISO/IEC 27002:2005)
LST ISO/IEC 27005:2008	Informacijos saugumo rizikos valdymas (tapatus ISO/IEC 27005:2008)
LST ISO/IEC 27006:2007	Reikalavimai, keliami įstaigoms, atliekančioms auditą ir sertifikuojančioms

	informacijos saugumo valdymo sistemas (tapatus ISO/IEC 27006:2007)
LST ISO/IEC TR 18044:2007	Informacijos saugumo incidentų valdymas (tapatus ISO/IEC TR 18044:2004)

Standartai nuolatos tobulinami, koreguojami ir papildomi, prie jo kūrimo ir tobulinimo prisidėjo daug valstybinių ir komercinių organizacijų Didžiojoje Britanijoje ir kitose šalyse. Todėl šio darbo rezultatas yra pats išsamiausias, nuolat atnaujinamas informacijos apsaugos priemonių rinkinys. Atskirai įmonei nėra būtina naudoti visų juose išvardytų informacijos apsaugos priemonių. Tačiau, siekiant užtikrinti reikiamą informacijos apsaugos lygį, reikėtų peržiūrėti visas standartuose išvardytas apsaugos priemonės ir, jeigu kuri nors iš priemonių nėra naudojama, turi būti žinoma, dėl kokių priežasčių ji nenaudojama.

1.2.1. Pagrindiniai informacijos saugos standartai

Informacijos saugos standartai yra skirti organizacijos informacijos saugumo patikrai. Jie gali būti skirstomi pagal tai, kaip jie yra taikomi. Kai kurie standartai yra tarptautinio pobūdžio, kiti yra paskelbti šalies vyriausybių, dar kiti yra sukurti profesionalių organizacijų kaip profesionalios praktikos standartai, dar vadinami organizaciniais standartais.

Egzistuoja įvairių bendrųjų tarptautinių standartų, tiek daugiau techniniai, tiek labiau abstraktūs. Pavyzdžiui, abstraktus yra OECD Guidelines [3]. Jis naudojamas organizacijai siekiant sukurti tinkamą saugos kultūrą, ir nurodo kryptį teisės aktams.

Organizaciniai standartai ir gairės yra detalesni, orientuoti į tam tikrą sritį. Jie naudojami užtikrinti dar geresnę saugą. Vienas svarbiausių ir dažnai naudojamų yra COBIT standartas (Control Objectives for Information and related Technology) [3]. Tai yra kontrolinė sistema, kuri sieja IT su verslo reikalavimais, sutelkia IT veiklą į bendrai pripažintą procesų modelį, identifikuoja pagrindinius IT resursus ir apibūdina valdymo kontrolės tikslus, kurių turi būti laikomasi. Jis sukurtas IT Governance instituto (ITGI) 1995 metais ir periodiškai atnaujinamas. COBIT yra priimtas tarptautiniu mastu kaip gairės, skirtos IT valdymui, kurios leidžia vadovams susieti ir suderinti kontrolės reikalavimus, technines priemones ir verslo riziką. Jis lengvai taikomas mažoms ir vidutinio dydžio organizacijoms [7].

IT Infrastructure Library (ITIL) talpina integruotą ir procesais paremtą geriausią praktikos rinkinį informacinių technologijų paslaugų valdymui. Yra aiškiai apibrėžti kokybiniai ir ekonominio efektyvumo tikslai, reikalingi teikiant IT paslaugas. ITIL apima apsaugos sritis, tokias kaip politika, procesai, procedūros ir darbo instrukcijos.

ISF (The Information Security Forum), tai informacijos saugos standartas, kuris aprašo visą informacijos saugos praktiką organizacijoje. Šis standartas aprašo informacijos saugą iš verslo perspektyvos ir suteikia praktinį pagrindą įvertinti organizacijos informacijos saugumo priemones. Šis standartas sukurtas 1996 metais ir yra atnaujinamas bent kartą per dvejus metus, siekiant patenkinti pirmaujančių tarptautinių organizacijų poreikius, patikslinti informacijos saugumo sritis, suderinti su kitais su informacijos saugumu susijusiais standartais (ISO 27002 (17799), COBIT v4.1 ir PCI / DSS) [18]. ISF standartas yra viešai prieinamas dokumentas, išskirstytas į 6 raktines sritis [18]:

- Kompiuterių įrengimas
- Saugos valdymas
- Ypatingos svarbos verslo taikomųjų programų naudojimą
- Tinklų kūrimas
- Sistemų kūrimas
- Galutinio vartotojo aplinka

Yra sukurta įvairių nacionalinių IT saugos standartų. Jis sukurti kaip privalomi saugos reikalavimai atitinkamose valstybinėse įstaigose. Tokių standartų pavyzdžiai yra: Australian Communications Security Instructions numeris 33 (ACSI33), kuriame nurodytos gairės Australijos standartas valstybinių įstaigų IT sistemų saugai; Vokietijos federalinės agentūros IT saugos standartas German IT Baseline Protection Manual; US NIST 800 - JAV nacionalinio standartų ir technologijų instituto sukurtas IT saugos standartas [3].

NIST SP800 standartų grupė buvo įkurta 1990 metais. Ji susideda iš daugiau nei šimto dokumentų, apimančių beveik visus informacijos saugos aspektus. Vienas svarbiausių yra SP8000-12 standartas. Tai vartotojo vadovas, išsamiai apimantis pagrindinius informacijos saugos principus. Išskiriami 8 pagrindiniai elementai [27]:

1. Kompiuterių saugumas turi būti paremtas organizacijos misija
2. Kompiuterių saugumas yra svarbiausias veiksnys siekiant patikimo valdymo
3. Kompiuterių saugumas turi būti ekonomiškai efektyvus.
4. Turi būti aiškiai apibrėžta saugi prieiga ir atsakomybės.
5. Sistemos savininkai turi nešti atsakomybę už išorinę saugą.
6. Kompiuterių saugumas reikalauja visapusiško ir integruoto požiūrio.
7. Kompiuterių saugumas turi būti periodiškai peržiūrimas ir papildomas.
8. Kompiuterių saugumas yra ribojamas socialinių veiksnių.

2 lentelėje pateikti dažniausiai naudojami IS saugos standartai [2, 3, 7, 19, 21, 25, 27]:

2 lentelė. Dažniausiai naudojami IS saugos standartai

Standarto tipas	Standartas	Paskirtis	Skirti vartotojams
Tarptautiniai standartai	ISO/IEC 27002	Standartas, talpinantis dešimties saugos sričių informacijos saugos valdymo praktiką ir aprašo praktines gaires organizacijos saugos standartų kūrimui.	Darbuotojams, atsakingiems už informacijos saugą
	ISO/IEC 27001	Standartas, kuriame nurodomi reikalavimai įgyvendinti, valdyti, stebėti, analizuoti, palaikyti ir gerinti dokumentuotą informacijos saugumo valdymo sistemą (ISMS). Naudojamas siekiant ISMS sertifikato.	Darbuotojams, atsakingiems už informacijos saugą, auditoriams
	ISO/IEC 15408	Standartas, geriau žinomas kaip CC (Common Criteria). Jis padeda įvertinti, patvirtinti ir sertifikuoti technologinių produktų saugumo patikimumą nuo daugelio veiksnių.	Vartotojams, kūrėjams ir vertintojams
	ISO/IEC 13335	Standartas yra techninei saugos kontrolei skirtų priemonių rinkinys.	Aukštesnio lygio vadovams ir darbuotojams, atsakingiems už saugos priemones
	OECD Guidelines	Standartas, kuriame nurodomos gairės siekiant sukurti tinkamą saugumo kultūrą organizacijoje.	Aukštesnio lygio vadovams
Organizaciniai standartai ar gairės	COBIT	Aprašo geriausią praktiką informacinių sistemų valdymo srityje.	Vadovams, auditoriams
	ITIL	Verslo valdymo teorija, orientuota į darbo procesų optimizaciją ir kokybės užtikrinimą IT sektoriaus bendrovėse.	Darbuotojams, atsakingiems už IT paslaugų valdymą
	ISF	Aprašo informacijos saugą iš verslo perspektyvos ir suteikia praktinį pagrindą įvertinti organizacijos informacijos saugumo priemones	Vadovams, atsakingiems už IT saugą, auditoriams, sistemų kūrėjams
Nacionaliniai standartai	ACSI 33	Standartas, kuriame nurodytos gairės Australijos valstybinių įstaigų IT sistemų saugai.	Darbuotojai, atsakingi už IT saugumą valstybinėse organizacijose
	BS 7799	Didžiosios Britanijos standartas, nustato saugumo valdymo sistemą, ir išsamias rekomendacijas saugumo politikai, pateikdamas apsaugos priemones ir kontrolės būdus.	Darbuotojai, atsakingi už IT saugumą valstybinėse organizacijose
	German IT Baseline Protection Manual	Vokietijos federalinės agentūros informacinių technologijų saugos standartas	Darbuotojai, atsakingi už IT saugumą valstybinėse organizacijose
	US NIST 800	JAV nacionalinio standartų ir technologijų instituto sukurtas IT saugos standartas	Darbuotojai, atsakingi už IT saugumą valstybinėse organizacijose

1.2.2. Tarptautinė standartų sistema ISO

Vieni iš labiausiai naudojamų yra ISO 27000 serijos standartai, turintys tarptautiniu mastu pripažintą vardą, ir yra plačiai naudojamas Lietuvoje atliekant informacijos saugos auditą. Šis standartas buvo parengtas tarptautinės standartizacijos organizacija (International Organization for Standardization). Ji buvo įkurta Ženevoje 1947 metais siekiant vystyti pasaulinius standartus, kurie aprašytų praktikas pramonėje ir komercijoje [19]. Jos nariais tapo mokslininkai ir ekspertai surinkti iš įvairių mokslinių organizacijų. 2700 serijos standartai, skirti ISMS (informacijos saugos valdymo sistemos) kūrimui siekiant sertifikato, buvo paskelbti 2005 metais [2]. Pirmtaku laikomas ISO/IEC 17799 standartas, kuris pasirodė 2000 m. ISO/IEC 17799 standartas buvo parengtas remiantis nacionaliniu Didžiosios Britanijos standartu BS 7799. Visi 2700 šeimos standartai atvaizduoti 1 paveiksle [2].

1 pav. ISO 27000 šeimos standartų struktūra

Pagrindiniai ISO standartai:

- **ISO/IEC 27002** – (pakeistas iš ISO/IEC 17799 2005 metais) yra tarptautinis standartas, nurodantis praktines rekomendacijas informacijos saugos valdymui bei praktines gaires, organizacinių saugumo standartų kūrimui ir valdymui šiom

apsaugos sritims [19]: (a) saugumo politika; (b) informacijos saugos organizavimas; (c) turto valdymas; (d) žmogiškų išteklių sauga; (e) fizinė ir aplinkos sauga; (f) ryšių ir operacijų valdymas; (g) prieigos kontrolė; (h) informacinių sistemų įsigijimas, kūrimas ir priežiūra; (i) informacijos saugos incidentų valymas; (j) veiklos tęstinumo valdymas; (k) Technikinių bei teisinių reikalavimų laikymasis. Tarp šių 10 apsaugos sričių yra 39 kontrolės tikslai ir šimtai geros praktikos informacijos saugos kontrolės priemonių, kurias rekomenduojama naudoti organizacijoms, atliekant kontrolės veiksmus ir apsaugant turtą nuo grėsmės informacijos konfidencialumui, vientisumui ir prieinamumui [3].

- **ISO/IEC 27001 –** yra tarptautinis standartas, kuriame apibrėžiami reikalavimai, kurie reikalingi, įgyvendinant, stebint, analizuojant, palaikant ir gerinant dokumentuotą informacijos saugos valymo sistemą (ISMS) organizacijoje. Šis standartas taikomas visiems organizacijų tipams, įskaitant verslo įmonės, valstybines organizacijas ir pan. Šiame standarte aprašomas ciklinis modelis „Plan-Do-Check-Act (PDCA) modelis, kuriuo siekiama sukurti, įgyvendinti, stebėti ir gerinti ISMS veiksmingumą organizacijoje [3]. Dažnai ISO/IEC 27001 yra įgyvendinamas kartu su ISO/IEC 27002. Nes ISO/IEC 27001 apibrėžia ISMS reikalavimus, o ISO/IEC 27002 nurodoma tinkamiausia informacijos saugumo kontrolė [19].
- **ISO/IEC 15408** – yra tarptautinis standartas, kitaip žinomas kaip “Common Criteria” (CC). Jis susideda iš trijų dalių: ISO / IEC 15408-1 (Įvadas ir bendras modelis), ISO / IEC 15408-2 (saugumo funkciniai reikalavimai) ir ISO / IEC 15408-3 (saugumo užtikrinimo reikalavimus) [3]. Šis standartas padeda įvertinti, technologinių produktų saugą, juos patvirtinti ir, naudojant įvairius faktorius, tokius kaip saugos funkciniai reikalavimai, apibrėžti standarte.
- **ISO/IEC 13335** – standartas susideda iš 4 dalių, kuriose aprašomi techninių saugumo kontrolės priemonių gairės, informacijos ir ryšių technologijų saugumo modeliai ir koncepcijos, IT valdymo būdai, saugos priemonių paskirtis, tinklų saugumo valdymo gairės [3].

1.2.3. Informacijos saugos auditą reglamentuojantys standartai ir dokumentai

Informacijos saugos auditui atlikti reikalingi profesionalūs įgūdžiai ir patikimumas, tai neatsiejama nuo standartų, kurie turi būti naudojant atliekant informacijos saugos auditą. Standartai, procedūros ir gairės yra išduodami įvairių institucijų, kurios svarsto, kokiu būtų auditorius turėtų atlikti informacijos saugos auditą.

Informacijos saugos audito standartai numato daugelio lygių gaires. ***Standartai*** aprašo visų audito procedūros sričių schemą ir auditoriams ir nurodo reikalavimus audito sistemai. Jie apibrėžia auditorių atsakomybę ir užtikrina auditorių kompetenciją, patikimumą, objektyvumą ir savarankiškumą, bei dalyvavimą planuojant, atliekant ir pateikiant darbo ataskaitas. ***Gairės*** pateikia rekomendacijas IS audito standartų taikyme. IS auditorius, įgyvendindamas standartus, turi apsvarstyti gaires, kaip jie bus įgyvendinti, pasinaudoti profesionaliu sprendimu ir turi būti pasirengęs pagrįsti vieną ar kitą veiksmą. ***Procedūros*** pateikia procedūrų pavyzdžius, kuriais IS auditorius turi vadovautis vykdant auditą. Jose pateikiama informacija apie tai, kaip atitikti standartams vykdant IS auditą, bet tai nėra reikalavimai. IS audito gairių ir procedūrų tikslas yra pateikti daugiau informacijos apie tai, kaip laikomasi IS audito standartų [25].

Atlikdamas IS auditą auditorius turi atsižvelgti į konfidencialumą, vientisumą ir prieinamumą, ir atlikdamas darbą jis turi vadovautis tarptautiniais ar atitinkamais nacionaliniais standartais. Pavyzdžiui: INTOSAI audito standartai, International Federation of Accountants (IFAC) audito standartai, tarptautiniai standartais profesionalių audito institucijų, tokių kaip Information Systems Audit and Control Association (ISACA) ir Institute of Internal auditors (IIA) [21]. 3 lentelėje pateikta detali informacija apie organizacijas, formuojančias standartus, gaires ar procedūras IS auditui.

3 lentelė. Organizacijos, formuojančios standartus, gaires ar procedūras IS auditui

Organizacija	Organizacijos pavadinimas	Dalyvavimas IS audite	Ryšiai su Lietuva
INTOSAI	Tarptautinės aukščiausiųjų audito institucijų organizacija	Rengia audito standartus. IT audito darbo grupė rengia gaires IT auditui.	Nuo 1992 metų Lietuvos Valstybės kontrolė yra INTOSAI narė.
IFAC	Tarptautinė apskaitininkų federacija	Rengia tarptautinius audito standartus. Rengia tarptautines metodikas IT auditui.	Nuo 2003 metų Lietuvos auditorių rūmai yra IFAC narys.
ISACA	Informacinių sistemų audito ir valdymo asociacija	Rengia standartus, kurie padeda nustatyti IS audito ir ataskaitų rengimo privalomuosius reikalavimus, bei IS audito standartų taikymo metodikas ir audito veiklos procedūras.	2002 metais įsteigtas ISACA Lietuva skyrius.
IIA	Vidaus auditorių	Rengia IS audito standartams	1997 metais įsteigtas IIA

	asociacija	papildomas metodines rekomendacijas.	skyrius Lietuvoje.
ISO	Tarptautinė standartizacijos organizacija	Rengia tarptautinius IS standartus. Rengia gaires IS auditui.	Nuo 1996 metų Lietuvos standartizacijos departamentas yra ISO narys.

ISACA paruošė eilę standartų IT auditoriams iš skirtingų IT sričių. Tam, kad IT auditoriai galėtų sekti audito standartais ISACA taip pat išleido audito gaires, kurios nurodo kryptį audito standartams. Kelios svarbiausių ir naudingiausių IT auditoriams gairių pateiktos 4 lentelėje [21].

4 lentelė. ISACA svarbiausios gairės IT auditui

Gairės	Tikslas
060.020.020 Taikomųjų sistemų apžvalga	Aprašo rekomendacijas atlikti taikomųjų programų apžvalgai.
060.020.060 IS valdymo efektyvumas	Aprašo gaires, naudojamas atliekant IS valdymo efektyvumo vertinimą organizacijoje.
060.020.070 Kompiuterinių audito metodų naudojimas (CAATs)	Aprašo gaires kaip naudotis CAAT, kuris yra svarbus įrankis IT auditoriams atliekant auditą.

ISACA nustatė visų kategorijų IS auditui taikomus šiuos bendruosius reikalavimus [7]:

1. IS audito funkcijų atsakomybė, įgaliojimai ir atskaitomybė turi būti tinkamai dokumentuoti;
2. IS auditorius turi būti nepriklausomas nuo audituojamos organizacijos;
3. IS auditorius turi laikytis profesinės etikos kodekso. Auditas turi būti įgyvendintas laikantis profesionalių audito standartų;
4. IS auditorius turi būti techniškai kompetetingas, turėti įgūdžių ir žinių, reikalingų atlikti auditą ir turi išlaikyti bei didinti techninę kompetenciją atliekant profesinį mokymąsi;
5. IS auditorius turi planuoti savo darbą;
6. IS audito grupės nariai turi būti tinkamai prižiūrimi taip, siekiant užtikrinti, kad yra laikomasi audito tikslų ir taikomi audito standartai. Audito duomenys ir išvados turi būti paremtos tinkama analize ir pateikta pakankama, patikima, naudinga ir reikalinga informacija;
7. Atlikus auditą IS auditorius turi pateikti gavėjams ataskaitą, iš anksto apibrėžta forma;
8. IS auditorius, praėjus numatytam laikui po IS audito atlikimo turi patikrinti audito metu gautas išvadas.

5 lentelėje pateikti tarptautiniai audito standartai ir tarptautiniai audito praktikos pareiškimai, kurie sukurti IFAC [21]:

5 lentelė. IFAC standartai ir geirės IT auditui

Standartas/Gairės	Tikslas
ISA 400 Rizikos vertinimas ir vidaus kontrolė	Nustato standartus ir pateikia gaires, kaip vertinti vidaus kontrolės struktūrą ir audito riziką bei jos komponentus: vidinę riziką, kontrolės riziką ir aptikimo riziką.
ISA 401 Kompiuterinių informacinių sistemų aplinkos auditas	Nustato standartus ir pateikia gaires kompiuterinių informacinių sistemų aplinkos auditui.
ISA 600 Kitų auditorių darbo panaudojimas	Nustato standartus ir pateikia gaires auditui, kai auditas vykdomas pasinaudojant buvusio audito ataskaitomis.
ISA 610 Vidinio audito darbo vertinimas	Nustato standartus ir pateikia gaires išorės auditoriams, kaip vertinti vidinio audito veiklą ir nustatyti poveikį audito rizikai.
IAPS 1001 IT aplinka – pavieniai asmeniniai kompiuteriai	Aprašo PC įtaką skaičiavimo sistemoms ir susijusiems vidiniams kontrolės mechanizmams bei audito procedūroms.
IAPS 1002 IT aplinka – On-Line kompiuterių sistemos	Aprašo on-line kompiuterių įtaką skaičiavimo sistemoms ir susijusiems vidiniams kontrolės mechanizmams bei audito procedūroms.
IAPS 1003 IT aplinka – duomenų bazių sistemos	Aprašo duomenų bazių sistemų įtaką skaičiavimo sistemoms ir susijusiems vidiniams kontrolės mechanizmams bei audito procedūroms.

ISO susiję su IS auditu standartai pateikti 6 lentelėje [21].

6 lentelė. ISO standartai IS auditui

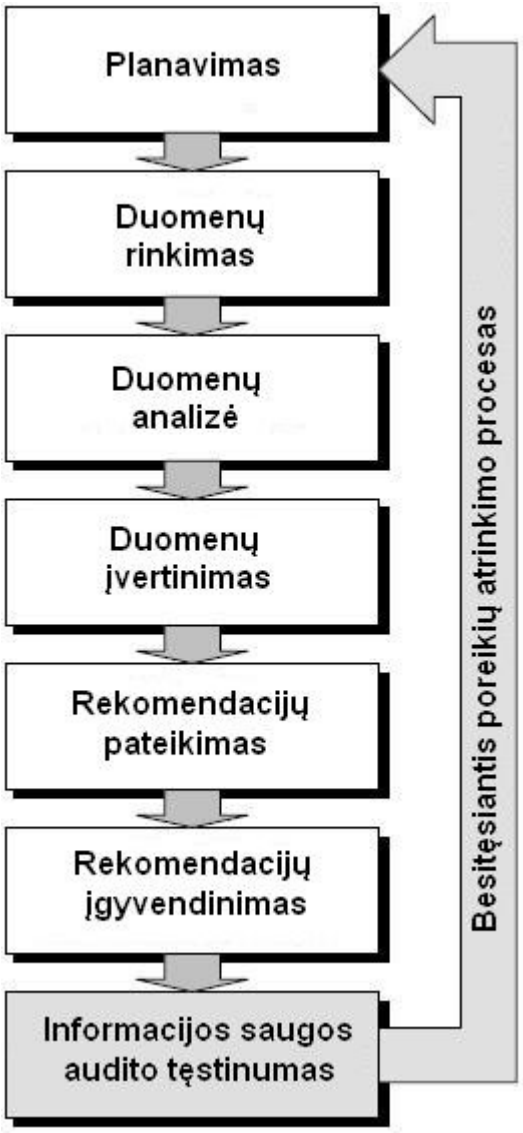
Standartas/Gairės	Tikslas
ISO 19011	Gairės kokybės valdymo sistemų auditui ir aplinkos valdymo sistemų auditui
ISO 27006	Reikalavimai, keliami įstaigoms, atliekančioms auditą ir sertifikuojančioms informacijos saugumo valdymo sistemas
ISO 27007	Gairės informacijos saugos valdymo sistemų auditui.

1.3. Informacijos saugos audito procedūra

Informacijos saugos audito įgyvendinimą galima suskirstyti į 7 etapus [15]:

1. Planavimas
2. Duomenų rinkimas
3. Duomenų analizė
4. Duomenų įvertinimas
5. Rekomendacijų pateikimas
6. Rekomendacijų įgyvendinimas
7. Informacijos audito tęstinumas

Pateiktas modelis nėra gerai struktūrizuotas ir kontroliuojamas procesas, kuris griežtai turi būti taikomas visais atvejais. Tai tik pagrindas, nes auditas yra lankstus procesas, ir kiekvienu atveju yra keliami skirtingi reikalavimai ir apribojimai organizacijai.



2 pav. Informacijos saugos audito įgyvendinimo etapai

Planavimas. Kaip ir bet kokiam projekte planavimo etapas yra labai svarbus, jame galime nustatyti projekto sėkmę ar nesėkmę. Norint tinkamai suplanuoti, reikia atlikti 5 žingsnius [15]:

1. Suprasti savo organizaciją ir parengti aiškius tikslus
2. Nustatyti taikymo sritį ir paskirstyti išteklius
3. Pasirinkti metodologiją
4. Sukurti komunikavimo strategiją
5. Pritraukti vadovų paramą

Audito duomenų rinkimas. Duomenys gali būti renkami:

- klausimyno pagalba arba vykdant asmeninius pokalbius.
- susitikime su organizacijos atstovais jie pateikia organizacinius ir techninius dokumentus, tokius kaip struktūriniai organizacijos dokumentai, pagrindinės IT koncepcijos, atsakomybių grafikas, saugos politikos dokumentas, sąrašas kritinių biznio procesų, ankstesnių buvusių informacijos saugos audito rezultatų dokumento (jei auditas buvo atliekamas)[16].

Taip pat turi būti griežtai apibrėžti audito objektai, įskaitant bendrą organizacijos aprašymą (vietą, biurų skaičių, darbuotojų skaičių, užduočių/tikslų skaičių organizacijoje), įvardinti pagrindiniai organizacijos uždaviniai ir procesai informacijos, kuri bus egzaminuojama [17].

Duomenų analizė. Analizės procesas nustato spragas, dubliavimus, lyginama su nuostatais, standartais. Nustatoma duomenų svarba ir kritiniai duomenys pažymimi. Analizė gali būti daroma vidinė arba išorės analitikų atsižvelgiant į jos sudėtingumą ir surinktų duomenų apimtį. Taip pat yra įvairiausių kompiuterizuotų priemonių, palengvinančių analizės procesus.

Analizė gali būti trijų rūšių: bendroji, strateginės reikšmės analizė ir informacijos srautų žemėlapių sudarymas [15].

Bendrosios analizės atveju surinkti bet kokių atvirų klausimų duomenys analizuojami bendrai, naudojant skaičiuokles arba duomenų bazės programas arba naudojant specialius analizės įrankius.

Strateginės reikšmės analizė atliekama naudojantis informacinių išteklių duomenų baze. Duomenų bazė gali būti naudojama siekiant atlikti informacijos ir žinių inventorizaciją. Informacijos išteklių duomenų bazė gali būti naudojama siekiant generuoti ataskaitas.

Informacijos srautų žemėlapių sudarymo analizės metodas analizuoja informacijos srautus įmonės viduje ir išorėje, sudaro žinių perdavimo modelį.

Galimi keli informacijos saugos audito duomenų analizės būdai [33]:

- Auditorius, remdamasis rizikų analizės metodu, apibrėžia tiriamai sistemai individualų saugos reikalavimų rinkinį, labiausiai įvertinantį duotosios sistemos ypatybes, jos funkcionavimo aplinką ir šioje aplinkoje esančias saugos grėsmes .
- Pagrįstas informacijos saugos standartais, kurie apibrėžia plačios informacinių sistemų klasės saugos reikalavimus, kurie formuojami apibendrinant pasaulinę praktiką. Auditoriui šiuo atveju reikia teisingai nustatyti standarto reikalavimų rinkinį, kurį turi

atitikti duotoji informacinė sistema, ir parinkti metodiką, įvertinti šiam atitikimui. Tai labiausiai paplitusi audito metodika, kuri leidžia su minimaliomis išlaidomis daryti pagrįstas išvadas apie informacinės sistemos būklę.

- Dviejų pirmųjų būdų kombinacija, kai informacinės sistemos saugos bazinių reikalavimų rinkinys nustatomas standartu, o papildomi reikalavimai, įvertinantys duotos informacinės sistemos funkcionavimo ypatybes, formuojami rizikų analizė pagrindu.

Duomenų įvertinimas. Kiekvienai problemai, kuri yra nustatoma gali būti daugiau nei vienas sprendimas ir yra svarbu, kad būtų rekomenduojamas tinkamiausias sprendimas. Sprendimo tinkamumui įvertini turi būti naudojama svarbumo vertinimo sistema [15]. Svarbu, kad rekomendacijos suformuluotos šiame etape būtų realios, pasiekiamos ir valdomos. Išlaidas, susijusias su rekomendacijomis, įgyvendinimo procesai ir kiekybiniai tikslai turi būti nustatyti ir patvirtinti dokumentais [16].

Rekomendacijų pateikimas. Visame audito procese labai svarbi yra bendravimas. Nemažiau svarbu tai, kas po rekomendacijų buvo suformuluota. Kadangi daugelis rekomendacijų liečia išteklius ir paslaugų organizavimą, tai jos gali įtakoti daugelio darbuotojų kasdieniam darbo procesui. Labai svarbu, kad vykdomi pakeitimai būtų pateikiami darbuotojams kaip teigiami procesai, kurie užtikrins paramą jiems patiems. Tokiu būtu išlaikomi sėkmingi komunikavimo kanalai viso audito proceso metu ir darbuotojai lieka patenkinti audito procesu. Labiausiai paplitę metodai, kuriais perduodamos rekomendacijos yra rašytiniai pranešimai ir pareiškimai žodžiu susirinkimo metu. Kiti galimi metodai yra pateikti seminaruose, vidiniuose įmonės informaciniuose leidiniuose arba vidinėje internetinėje svetainėje. [15]

Rekomendacijų įgyvendinimas. Pateikus rekomendacijas yra parengiamas veiksmų planas jų įgyvendinimui bei nurodoma, kaip tai paveiks organizacijos informacijos saugą.

Informacijos audito tęstinumas. Informacijos auditas nėra baigtinis procesas. Kai įgyvendinamas jo pirmas etapas, jau jame yra numatoma antro etapo uždaviniai ir kada jie turi būti atliekami.

Visame informacijos saugos audito procese daugiausiai kompetencijos ir žinių reikalauja duomenų analizės ir duomenų įvertinimo etapai. Informacijos saugos auditorius turi turėti atitinkamas priemones, gebėjimus, metodus ir praktiką, kartu su atitinkamai parinktai techniniais organizacijos darbuotojais turi apsirašyti techninę įrangą (teikiančią tinko, interneto ir intraneto ryšį), programinę įrangą ir programas, kurios ir sudarys audito aplinką [17]. Auditorius ar auditoriai turėtų parengti aprašą identifikuotos infrastruktūros elementų, kurie bus nuolatos

atnaujinami, nes kompiuterinės sistemos yra kintančios. Iš auditoriaus reikalaujama ir gerų analitinių sugebėjimų duomenų analizei atlikti bei plačios apimties informacinių technologijų žinių, tiek iš techninės, tiek iš programinės, tiek iš valdymo srities.

1.4. Informacijos saugos audito atlikimo metodai ir įrankiai

Informacijos saugos auditą, kaip ir kitokio tipo auditą, auditoriai ar auditorių grupė gali atlikti dviem būdais:

- naudojantis automatizuotomis priemonėmis;
- nenaudojant automatizuotų priemonių (tradiciniu būdu).

Tai, kokių būdu bus atliktas auditas priklauso nuo auditorių turimų automatizuotų priemonių rinkinio bei žinių. Tradiciniu būdu atliekat auditą duomenų rinkimo etapas vykdomas tiesioginio susitikimo su organziacijos darbuotojais metu, jiems pateikiant klausimų anketas, arba jei yra tiriamas sistemų saugumas, tai atliekamos rankomis operacijomis, tokiu būtų bandant paveikti techninę ar programinę įrangą. Surinkta informacija taip pat nenaudojant automatizuotų priemonių yra vertinama ir pateikiami rezultatai remiantis audtoriaus, dažniausiai jų grupės patirtimi.

Automatizuotas auditas gali būti vykdomas naudojant įvairias automatizuotas priemones. Tai gali būti įrankis, skirtas saugos audito duomenų surinkimui, audito duomenų analizei, bei rezultatų pateikimui.

Rankiniu būdų vykdomas auditas yra mažiau efektyvus ir ilgas procesas, todėl sių laikų procese turėtų būti kuo labiau automatizuojamas.

Atliekant informacijos saugos audito automatizavimą dažniausiai yra naudojamos žiniomis paremtos sistemos, kurios veikia jau paruoštais klausimų ruošiniais, o galimų atsakymų analizės priemonės pateikia rezultatus ar rekomendacijas. Jos skirtos auditoriaus darbo supaprastinimui. Viena iš tokių yra „Cobra“.

„Cobra“, tai rizikų valdymo sistema, skirta paprastai nustatyti organizacijos rizikoms ir jas kontroliuoti. Ji yra taisyklėmis paremta ekspertinė sistema, kur vartotojas turi atsakyti į eilę klausimų, po kurių yra pateikiami rezultatai ir rezultatų ataskaitos [8]. Taip pat jis turi draugišką vartotojo aplinką, bei galimybę rezultatus konvertuoti į MS Word formatą. Naudodama savo didele žinių baze sistema nustato grėsmes, pažeidžiamumus ir poveikį saugumui. Taip pat sistema talpina didelį klausimyną, kuris sukurtas suderinant su ISO17799/BS7799 standartais [8]. Taigi „Cobra“ suteikia galimybę atlikti išsamią rizikos analizę atitikimui standartams.

Kita mokama sistema Security Decisions 2007 [31]. Skirta organizacijoms, naudojančioms savo veikloje informacines technologijas. Joje talpinami problemų sprendimai ir su išsamiu aprašymu. Sistema pasiūlo sprendimą tam tikrai problemai, ir suteikia galimybę vartotojui pateikti savo problemos sprendimo versiją. Tačiau ji neatlieka rizikos įvertinimo, o tik talpina nemažą informacinę bazę.

AMS9000 mokama audito valdymo programinė įranga, skirta informacijos saugos auditui atlikti pagal ISO 27001 standartą [1]. Talpina klausimyną, parengtą pagal šiuos standartus ir leidžia pildyti klausimyną savo klausimais. Taip pat leidžiamas sudaryti audito planą, bei saugoti buvusių auditų duomenis, bei teikia audito ataskaitas. Programa neturi sprendimų priėmimo galimybių.

Callio Secura 17799 – mokamas auditui skirtas įrankis, pritaikytas auditui pagal ISO 17799 standartą [5]. Talpina savyje klausimyną ir leidžia kurti savo klausimyną, taip pat reguliuoti klausimų svorius. Atsakius į klausimus yra grafine forma pateikiamas rezultatas, kartu nurodant saugumo lygį organizacijoje.

7 lentelė. Automatizuoti įrankiai IS auditui

Automatizuotas įrankis	Paskirtis	Sprendimų/ rekomendacijų pateikimas	Rizikos vertinimas	Suderinamumas su standartais
Cobra	Rizikų valdymo sistema, skirta nustatyti saugos rizikoms ir jas kontroliuoti.	Taip	Taip	ISO 17799
Security Decisions 2007	Sistema, skirta sprendimų priėmėjams, talpina saugos sprendimų bazę.	Taip	Ne	Ne
AMS9000	Sistema skirta vidinio audito valdymui, aprašo audito procesą.	Ne	Taip	ISO 27001
Callio Secura 17799	Sistema skirta informacijos saugos valdymui organizacijoje, paruošia ISMS auditui.	Taip	Taip	ISO 17799
CounterMeasures	Sistema skirta nustatyti, vertinti ir valdyti IT rizikoms.	Taip	Taip	NIST 800

1.6. Automatizuotų audito sistemų realizavimo metodai

Įprastinėms problemoms spręsti kompiuterinės programos sprendimui rasti naudoja gerai struktūrizuotus algoritmus, duomenų struktūras ir sprendimų paieškos strategijas.

Tradicinės taisyklėmis pagrįstos sistemos naudoja žmogiškąsias ekspertines galimybes realioms problemoms spręsti, kurios dažniausiai reikalauja žmogaus intelekto. Ekspertinės žinos dažnai pateikiamos taisyklių forma.

Taisyklėmis paremtos sistemos vaidina svarbų vaidmenį moderniose intelektualiose sistemose. Jos naudojamos strateginių tikslų nustatyme, planavime, projektavime, diagnostikai, nesėkmių stebėjimui ir kt.

Įprastinės kompiuterinės programos, kurios naudoja sprendimų priėmimo logiką užduotims atlikti, apima labai nedaug žinių ir naudoja bazinius algoritmus specifinėms problemoms spręsti. Pagrindinės žinios yra dažnai įterpiamos į programinį kodą, kas reiškia, kad jei duomenys pasikeis, programa turės būti iš naujo perrašoma. Duomenimis paremtos ekspertinės sistemos renka nedidelius žmogaus žinių fragmentus ir saugo juos duomenų bazėje, kurios pagalba ieškomos problemos priežastys. Svarbus privalumas yra tas, kad ta pati žinių bazė gali būti naudojama sprendžiant skirtingas problemas neatliekant jokių programinių pakeitimų. Keli svarbiausi tokių sistemų privalumai:

- Sugebėjimas rinkti ir saugoti žmonių patirtį;
- Įgalina sukurti sistemą, kuri yra nuoseklesnė nei žmonių ekspertų mastymas;
- Sumažina žmogiškosios patirties poreikį;
- Sprendimas randamas greičiau nei žmonių ekspertų.

Tokios yra Sprendimų paramos sistemos (DSS – Decision Support Systems), kurios dalyvauja sprendimų priėmimo procese ir vartotojams padeda priimti sprendimus. Vykdydami žmogaus – mašinos pokalbį, jos gali teikti sprendimus. Trumpai tariant, tai kompiuterinė informacinė sistema, kuri gali padėti sprendimus priimantiems asmenims naudojantis duomenimis ir modeliais, spęsti nestruktūrizuotas arba dalinai struktūrizuotas problemas [9]. Nuo 1970-tųjų nagrinėjamos sprendimų paramos sistemos tapo pagrindine kompiuteriais paremtų informacinių sistemų dalimi.

9-ąjame dešimtmetyje pastebima informacinių technologijų banga – dirbtinio intelekto pagrindu paremtos ekspertinės sistemos (ES – Expert System), kurios pakeičia ir imituoja žmogaus sprendimų priėmimo proceso siauras sritis [29]. Apjungiant sprendimų paramos sistemas su ekspertinėmis sistemomis tampa lengviau spręsti sudėtingas dalinai struktūrizuotas ir nestruktūrizuotas problemas. Tokios sistemos vadinamos intelektualiomis sprendimų paramos sistemomis. 8 lentelėje pateikiamas sprendimų paramos ir ekspertinių sistemų palyginimas.

8 lentelė. DSS ir ES palyginimas

Sprendimų paramos sistemos (*DSS – Decision Support Systems*)	**Ekspertinės sistemos (*ES – Expert System*)**
Remiasi savo turimomis žiniomis, taisyklėmis ir išvadų generatoriais, pačios suformuoja ir pateikia sprendimą.	Sprendimų priėmėjui pateikia pagrįstus, dažniausiai kiekybinius argumentus sprendimui priimti, tam naudodama jai prieinamus informacinius ir kitokius išteklius.
Remiasi anksčiau įgytomis žiniomis ir taisyklėmis apie problemos sprendimą.	Palieka nemažai erdvės sprendėjo intuicijai, patirčiai, pasaulėžiūrai.
Pačios formuoja sprendimo trajektoriją.	Atlieka pasyvesnį pagalbinį vaidmenį, nors galimos situacijos, kai sprendimų paramos sistemos siūlo sprendimų priėmėjui tolesnius veiksmus.

9-to dešimtmečio viduryje vykdomosios informacinės sistemos (EIS – Executive Information Systems) tampa svarbi priemonė patenkinant informacijos poreikį. Naujausia versija yra dirbtiniai neuroniniai tinklai (ANN – Artificial Neural Networks). Neuroniniai tinklai savo funkcionalumu veikia reikalaudami tik minimalaus žmogiško įsikišimo. Dirbtinio intelekto sistemos, sukurtos imituoti žmogaus smegenų biologinės nervų sistemos veiklai: mokymąsi, mąstymą, informacijos saugojimą, atgaminimą ir atpažinimą. Taip pat dalyvauja kuriant pažangias sistemas, imituojančias žmogaus smegenų veiklą, remiasi patirtimi (t.y. mokosi iš savęs) ir greitai išgauna didžiulius duomenų kiekius. Neraiški logika, genetiniai algoritmai yra dalis kitų pažangių metodų, kurie naudojami kartu su neuroniniais tinklais tam, kad pagerintų asmeninį, grupinį ir organizacinį spendimų priėmimą.

1.7. Intelektualių sprendimų paramos sistemų realizavimo metodai

Remiantis įvairiais apibrėžimais DSS gali būti apibūdinama kaip kompiuterizuota interaktyvi žmonėms skirta kompiuterinė sprendimų priėmimo sistema, kuri [12]:

1. padeda spendimų priėmėjams, o ne pakeičia juos;

2. naudoja duomenis ir modelius;

3. išsprendžia problemas, susijusias su įvairia struktūra: (a) nestruktūruoti ar blogai struktūrizuoti, (b) dalinai struktūrizuoti; (c) struktūrizuoti;

4. palengvinant sprendimų priėmimo procesus.

Egzistuoja 4 tipų sprendimai: struktūrizuoti, dalinai struktūrizuoti, nestruktūrizuoti. Jie detaliau aprašyti aprašyti lentelėje Nr.9 [9, 11, 26].

9 lentelė. Sprendimų priėmimo klasifikacija

	Apibendrinimas	**Sprendėjai**	**Technologiniai panaudojimai**
Struktūrizuoti	Tiksliai ir griežtai apibrėžtų	Konkrečių funkcijų	Valdymo informacinės

sprendimai	taisyklių procedūros, kurios reikalingos pateikti nurodytam rezultatui, esant tam tikroms sąlygoms. Apibrėžti yra visi SPS architektūros komponentai	vykdytojai (vadybininkai ir kt.)	sistemos, transakcijų apdorojimas
Dalinai struktūrizuoti sprendimai	Apibrėžtų taisyklių procedūros, kurios turi nenumatytiems atvejams skirtą numanomą sprendimą, kuris nėra tiksliai apibrėžtas. Apibrėžti yra tik keli SPS architektūros komponentai	Analitikai, gamybos planuotojai, kreditų vertintojai, aukštesnio lygio vadybininkai.	Sprendimų paramos ir žinių valdymo sistemos
Nestruktūrizuoti sprendimai	Neegzistuoja apibrėžtos taisyklių procedūros, o iškilusiems nenumatytiems atvejams taikoma tik turima patirtis ir nusidaryta nuomonė. Nėra apibrėžtų SPS architektūros komponentų.	Organizacijos vadovai, priimantys svarbius sprendimus	Ekspertinės sistemos, intelektualios sprendimų paramos sistemos, žinių valdymo sistemos

1.7.1. Sprendimų paramos tikslai ir etapai

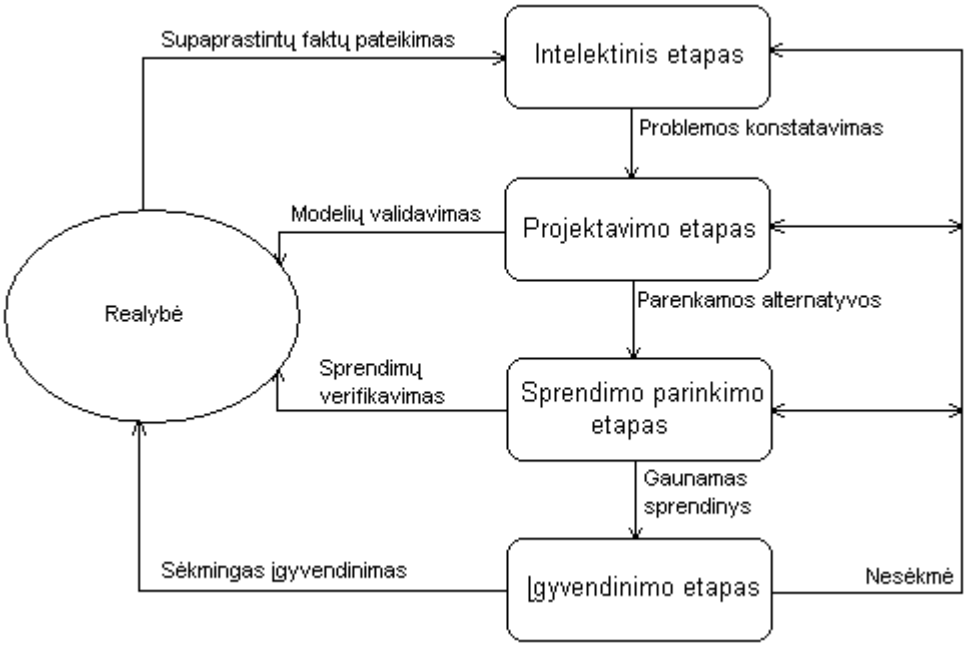
Pagrindiniai sprendimų paramos tikslai yra:

Nustatyti problemą – tai atliekama klausimų pagalbą. Vartotojui, šiuo atveju auditoriui, apie norimą problemą yra pateikiami klausimai, pagal kurių atsakymus sprendimų paramos sistema geba identifikuoti problemą naudodama Jei – Tai taisyklėmis. Taip surenka maksimalų informacijos kiekį apie esamą probleminę situaciją, kurios reikia problemai identifikuoti.

Pasiūlyti sprendimą – Identifikavus problemą yra integruotomis matematinėmis funkcijomis įvertinami rezultatų dydžiai ir pasiūlomas labiausiai tinkamas sprendimas.

Sprendimų paramos sistemos įtakoja visus sprendimo priėmimo proceso etapus [9, 11]:

- *intelektinį (intelligence)* – apima intelektualų problemos supaprastinimą, čia apibrėžiami organizaciniai tikslai, duomenų surinkimas, problemos identifikavimas, problemos klasifikavimas ir jos konstatavimas.
- *projektavimo (design)* – apima projekto modeliavimą, ieškomos ir formuojamos alternatyvos, numatomi ir įvertinami alternatyvų rezultatai
- *sprendimo parinkimo (choice)* – geriausios alternatyvos pasirinkimas tam tikromis sąlygomis, įgyvendinimo plano parengimas
- *įgyvendinimo (implementation)* – diegimas

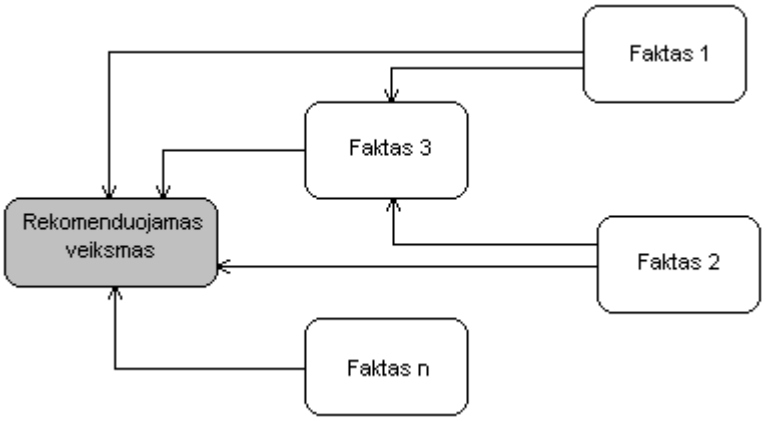


3 pav. SPS architektūros komponentai

Problemos identifikavimas yra pirmas procesas siekiant ją išspręsti ir įgyvendinti sprendimą. Taisyklėmis paremta sistema padeda identifikuoti problemos parametrus. Kad teisingai suformuoti problemą reikia ją atitinkamai išnagrinėti, pasinaudojant ekspertų žiniomis. Ir tik konstatavus problemą galima atlikti projektavimo etapą.

1.7.2. Tikslų struktūros modelis

Problemos identifikavimo etape yra formuojama priklausomybių diagrama, kuri atvaizduoja alternatyvias aplinkybes ar faktus, kurių kombinacija veda į išvadą [4]. Ji padeda žinių inžinieriui struktūrizuoti taisyklių grupes visai arba daliai žinių bazės. Rekomenduojamas veiksmas yra parenkamas pagal tam tikrus gautų sąlygų (faktų) rezultatus. Juos gali sudaryti ir vienas faktas, ir eilė faktų. Rekomenduojamas veiksmas bus tuo tikslesnis, kuo didesnis bus faktų bagažas, žinoma, priklausomai nuo problemos sudėtingumo. Priklausomybės diagramos pavyzdį reikia nagrinėti iš dešinės į kairę, nuo pradinių faktų link rekomenduojamų rezultatų.



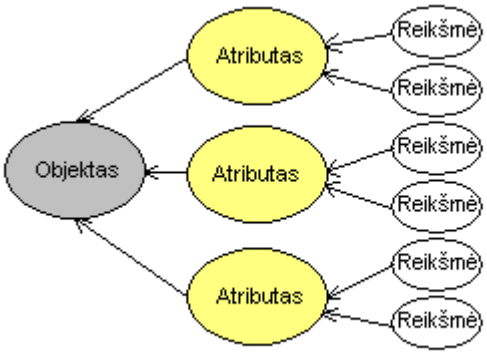
4 pav. Priklausomybių diagramos prototipas

Nebūtinai kelias iki rekomenduojamo veiksmo gali būti grįstas vien faktais. Keliaujant per faktus galima daryti tarpines išvadas, iš kurių po to formuojamas kitas faktas. Pvz.: diagramoje pavaizduoti Faktas 1 ir Faktas 2 veda į bendrą sprendimą, iš kurio formuojamas jau bendras Faktas 3, kuris apima gautą sprendimą.

Rekomenduojamą veiksmą galima pavadinti galutiniu tikslu, t.y. tikslas, kuris pasiekiamas einant per pradinius ir tarpinius tikslus (šiuo atveju faktus, nes faktas yra pasiektas tikslas). Apibendrinant galima teigti, kad priklausomybių diagramą sudaro tikslai ir ryšiai tarp jų. Taigi priklausomybių diagrama yra asimetrinis grafas, kuris neturi ciklų: $S=(G,R);$ čia $G=\{G_n|\ G_n$ – n-tasis tikslas$\}$, $n=1,...,N$. R yra visų ryšių tarp tikslų aibė [11]. Ryšių aibės elementai $R=\{r_{nl}|r_{nl} = (G_n,G_k),\ G_n$ – n-tasis tikslas $\}$. Kiekvienas ryšys $r_{nl} = (G_n,G_k),$ kur $k=1,..,K$ ir $n=1,..,K$. vaizduoja tiesioginį tikslo G_n įnašą siekiant tikslo G_k.

1.7.3. Objekto atributų reikšmių modelis

Projektavimo etape yra projektuojami modeliai, nustatomi pasirinkimo kriterijai, ieškomos ir formuojamos alternatyvos, numatomi ir įvertinami galimų alternatyvų rezultatai [11]. Tam šiame etape yra formuojamas objekto atributų reikšmių modelis (OAV) [4]. Sprendimų priėmimu paremtos sistemos surenka duomenis ir daro išvadas apie konkretų fizinį ar abstraktų objektą. Šie objektai turi vieną arba daugiau atributų ir kiekvienas atributas gali turėti vieną arba daugiau reikšmių.



5 pav. Objekto atributų reikšmių modelio prototipas (OAV)

Piešiant OAV modelius sprendimus priimančios sistemos aplinkoje dažnai susitelkiama į nagrinėjamos problemos struktūrą, kuri vėliau bus naudinga formuojant taisykles. Ekspertas turi padėti kurti OAV modelį ir turėtų sutikrinti informacijos tikslumą.

1.7.4. Sprendimų lentelės modelis

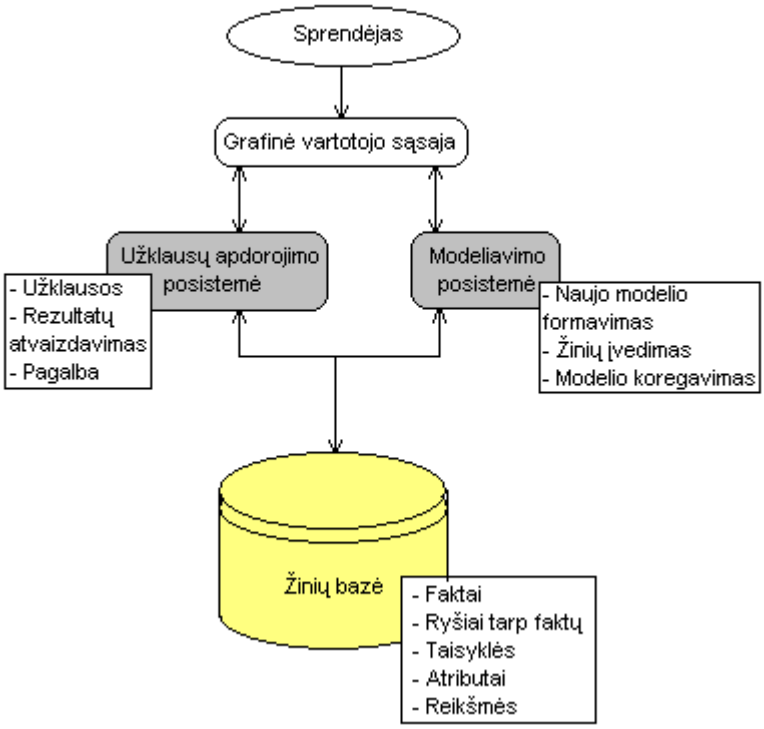
Sprendimų priėmimo taisyklės gali būti išreiškiamos per sprendimų lenteles [11]. Sprendimų lentelę sudaro sąlyga ir nebaigtinis sąrašas atributų, kurie vienaip ar kitaip daro įtaką sprendimui ir veiksmui, sudarančiam galimą sprendimą. Taisyklės yra užrašytos vertikaliai ir nurodo sąlygos atributus, kurie yra specifinio sprendimo rezultatas. Tokia lentelė gali būti labai didelė, priklausomai nuo nagrinėjamos problemos sudėtingumo ir galimų sąlygų ir veiksmų kiekio. Jei naudojamas neapibrėžtumas, tuomet naudojami ir svoriai išreikšti procentais arba kitokia išraiška [4]. Svorius turėti gali ir pati sąlyga, ir atvejis, ir veiksmas. 10 lentelėje yra pateiktas spendimų lentelės pavyzdys.

10 lentelė. Sprendimų lentelės pavyzdys

Taisyklė	Atvejis 1	Atvejis 2	Atvejis 3	Atvejis n
Sąlyga 1 100%	Taip 100%	Taip 20%	Ne 75%	
Sąlyga 2 90%	Taip 75%	Ne 100%	-	
Veiksmas 1 100%	X 100%	X 80%	X 32%	
Veiksmas 2 100%	X 45%	X 45%	X 90%	
Veiksmas 3 80%	X 75%	X 74%	X 40%	X 0%

1.8. Sprendimų paramos sistemos architektūra

Tipinė sprendimų paramos sistema susideda iš: žinių bazės, modeliavimo posistemės, užklausų apdorojimo posistemės bei grafinės vartotojo sąsajos [35]. Tokios sistemos architektūra pateikta 6 paveiksle.



6 pav. Tipinė sprendimų paramos sistemos architektūra

Užklausų apdorojimo posistemė – priima vartotojų užklausas, pateikia modeliavimo rezultatus ir pateikia paaiškinimus ir on-line pagalbą. Tai leidžia vartotojui gauti duomenis iš duomenų bazės kartu su duomenimis, gautais atliekant modeliavimo procesą ir pateikti juos įvairia forma. Pavyzdžiui lentelėmis. Ji taip pat leidžia vartotojui gauti meta informaciją apie duomenis ir modelius.

Modeliavimo posistemė – skirta padėti vartotojui kuriant modeliams. Sistema įgyja atitinkamas žinias per žinių įgijimo modulį. Jį sudaro meta duomenys naujiems duomenų rinkiniams, meta informacija apie naujus modelius ar struktūras, skirtas vartotojui problemai apibrėžti [9].

Automatinio modeliavimo modulis, esantis modeliavimo posistemėje, skirtas formuoti problemos modeliui. Po vartotojo užklausos problemos sprendimo pateikimui sistema surenka parametrus iš vartotojo apie tai, kaip ji turėtų būti išspręsta, ir įtraukia šiuos parametrus

formuluojant problemos modelį. Šitas procesas yra vadinamas automatiniu modeliavimu [35]. Kai problemos modelis yra suformuotas, sistema leidžia vartotojui jį koreguoti.

Žinių bazė talpina žinias apie duomenis. Žinių procesas remiasi žiniomis, kurios teikia vartotojui pagalbą problemų sprendimo procese. Bendrai, problemos sprendimo procesas apima problemos modelio formulavimą, modelio įvertinimą ir sprendimo formulavimą.

Tokioje sistemoje sprendimą priima sprendėjas, šiuo atveju auditorius. Kuris pagal pateiktus rezultatus, t.y. identifikuotą problemą, turi nuspręsti kokį sprendimą priimti nustatytai problemai išspręsti.

1.8.1. Žinių atvaizdavimas žinių bazėje [32]

Žinioms atvaizduoti žinių bazėje galima įvairiais būdais. Išskyriau 4 :

- Taisyklių formavimas
- Semantiniai tinklai
- Freimai
- Logika

Taisyklių formavimas (*Production Rules*). Tai tokia žinių atvaizdavimo forma žinių bazėje, kai ekspertų žinios yra apibrėžiamos JEI-TAI taisyklėmis. Kiekvienoje taisyklėje eilutė, kurioje aprašoma probleminė situacija (eilutė, kuri prasideda sąlyga „jei“ ir „ir“) yra vadinama taisyklės sąlyga. Eilutė, kurioje nurodyta, kokių veiksmų imtis nurodytoje situacijoje (eilutė, kuri prasideda „tai“) vadinama rezultatu.

Semantiniai tinklai (*Semantic Nets*). Tai tokia žinių bazės struktūros forma, kai grafiškai vaizduojamos žinios (objektai, sąvokos, situacijos, veikla), vadinamos mazgais, ir apjungiamos lankais, sukuriant ryšius tarp mazgų.

Freimai (*Frames*). Jie skirti atvaizduoti žinioms tokiame kontekste, kokiame tie objektai ir įvykiai atsiranda. Jie leidžia objektams paveldėti reikšmes iš kitų objektų. Be to, kiekvienas atributas gali turėti su juo susijusių procedūrų (vadinamų demonais), kurie vykdomi kai atributas yra iškviečiamas ar atnaujinamas.

Logika (*Logic*). Žinios atvaizduojamos kaip samprotavimas, kuris sudarytas iš dviejų prielaidų ir išvados, išplaukiančios iš kitų prielaidų. Logikos panaudojimas žinių atvaizdavimui žinių bazėje gali būti išskirtas į tris grupes: teiginių logika, pirmos eilės predikatų logika, ir neraiški logika.

Teiginių logika. Žinių bazė yra paremta simboliais, susietais tarpusavyje taip, kad atvaizduotų ekspertų žinias. Teiginių logika naudoja kintamuosius, kurie nurodo žinias. Šie kintamieji yra jungiami loginėmis jungtimis.

Predikatų logika. Naudojama neišbaigtoms žinioms atvaizduoti panaudojant kvantorius $\forall$ („visiems“) arba $\exists$ („kai kuriems“).

Neraiški logika. Naudojama ekspertų žinioms aprašyti, kai nėra žinomos tikslios vertės. Vienas iš metodų yra neraiškių aibių teorija (fuzzy set).

11 lentelė. Žinių atvaizdavimo žinių bazėje metodų palyginimas

Metodas	Savybės	Privalumai	Trūkumai

Taisyklių formavimas	• Dažniausiai naudojamas formuojant žinių bazę;
	• Kalbos sintaksei apibrėžti naudojama metakalba;
	• Turi aiškiai nustatytas formavimo taisykles;
	• Taisyklėms formuoti naudojami JEI-TAI sakiniai;
	• Ryšių medis yra grafinė forma;
	• Sprendimų paieškos strategija priklauso nuo kontroliavimo krypties:
	  • Tiesioginė grandinė
	  • Atgalinė grandinė
		• Paprasta, lengvai suprantama ir generuojama;
		• Nesudėtingas įgyvendinimas;
		• Egzistuoja formalūs aprašymai kaip pavyzdžiai;
		• Artima žmogaus kalbai.
			• Gali būti neefektyvus;
			• Kai kurios žinių formos nėra lengvai perteikiamos taisyklėse;
			• Esant dideliam taisyklių kiekiui gali būti sudėtinga jas suprasti ir valdyti.

Semantiniai tinklai	• Informacijos grafinis atvaizdavimas; • Sukurtas MR Quillian kaip žmogaus atminties modelį; • Ženklinimas kryptinis grafas; • Mazgus sudaro objektai arba situacijos; • Ženklai žymi vardą; • Mazgai gali būti objektai ar klasės; • Ryšiai atvaizduoja struktūrinę žinių informaciją; • Ženklai nurodo ryšių tipą; • OAV (object-attribute-value) modelis gali būti naudojamas charakterizuoti žinias.	• Paprastos ir veiksmingos žinių atvaizdavimo schemos (OAV modelis); • pateikiama detali informacija mazguose; • Galimas lengvas konvertavimas į kitą atvaizdavimo metodą; • Predikatų logika (mazgai atitinka kintamuosius arba konstantas); • Teiginių logika (mazgai ir ryšiai paverčiami kintamaisiais ir tinkamai sujungti loginėmis jungtimis).	• Nėra vidinės mazgų struktūros; • Galimi ryšiai tarp kelių mazgų; • Nėra paprasto metodo atvaizduoti euristinei informacijai; • Sudėtingas plėtimas; • Paprastoms problemos spręsti gali susidaryti dideli mazgų ir ryšių rinkiniai; • Labiausiai tinkamas binariniams ryšiams atvaizduoti; • Užklausos su neigiamais rezultatais gali būti nesėkmingos; • Trūksta standartų ryšių tipams.
Freimai	• Atvaizduoja susijusias žinias apie subjektą; • Naudoja daug reikšmių pagal nutylėjimą; • Rėmai yra hierarchinė struktūra; • Leidžia naudoti paveldėjimą	• Galimas reikšmių paveldėjimas; • Galimas reikšmių priskyrimas pagal nutylėjimą; • Gali gauti informaciją per susietas procedūras	• Nėra apibrėžtų standartų ryšiams, naudojamiems sieti bendruosius rėmus ir specifinius; • Reikšmės pagal nutylėjimą gali būti perrašomos, dėl to vienas esminis

	• Žinios paprastai sudaromas jungiant ryšiais priežastis ir pasekmes; • Susideda iš dviejų laukų: vadinamų „pėdsako vardo“ (slot name) ir „užpildo“ (filler); • „Pėdsakas“ gali nurodyti įvairių rūšių objektą: taisykles, faktus, nuotraukas, video informaciją, komentarą, klausimą, hipotezę ir kt.; • Kiekvienas atributas gali turėti su juo susijusių procedūrų (vadinamų demonais), kurie vykdomi kai atributas yra iškviečiamas ar atnaujinamas	(demonus); • Skirtingi objektai gali dalintis tuo pačiu rėmu; • Artima žmogaus žinių organizavimui.	atvaizdavimo tipas tampa neįmanomas – kad mišrus aprašymas šitų prasmių yra funkcijos struktūros ir jų dalių tarpusavio ryšiai; • Nutylėtas reikšmes gali tapti sudėtinga perrašyti, nes paveldėjimo funkcija žemesniame hierarchijos lygyje.
Logika (teiginių logika, predikatų logika, neraiški logika)	• Žinios atvaizduojamos kaip samprotavimas, kuris sudarytas iš dviejų prielaidų ir išvados, kuri išplaukia iš prielaidų; • Logikos panaudojimas žinių atvaizdavimui žinių bazėje gali būti išskirtas į tris grupes: teiginių logika, pirmos eilės predikatų logika, ir neraiški logika; • Teiginių logika naudojama atvaizduoti išskirtinėms ekspertų žinioms, kurių reikšmės yra visuomet tiesa; • Teiginių logika naudoja loginius kintamuosius atvaizduoti žinioms, jungiant kintamuosius loginėmis jungtimis; • Predikatų logika naudojama neišbaigtoms žinioms atvaizduoti, panaudojant kvantorius.	• Galima išreikšti žinias trim būdais: teiginių logika, pirmos eilės predikatų logika, ir neraiški logika; • Lengvai aprašomi neapibrėžtumai; • Žinioms aprašyti nereikia naudoti daug simbolių.	• Naudojami specifiniai simboliai, dėl ko sudėtinga jas išreikšti žinių bazėje; • Tik logika paremta žinių bazės struktūra nepalaiko standartinės pagal nutylėjimą sprendimo paieškos.

1.8.2. Taisyklėmis paremtos sistemos sprendimų paieškos strategija

Ekspertinės sistemos komponentas išvadų generatorius tam tikra tvarka apdoroja žinių bazėje esančias taisykles. Jis nurodo samprotavimų strategiją, t.y. taisyklių apdorojimo strategiją, kurias taisykles ir kokia tvarka vykdyti. Galimos dvi sprendimų paieškos strategijos [4, 32]:

- tiesioginės grandinės metodas;
- atgalinės grandinės metodas.

Tiesioginės grandinės metodas. Dirbant tiesioginės grandinės metodu iškeliama taisyklė. Jos rezultatas saugomas darbinėje atmintyje ir ieškoma taisyklių bazėje kitos taisyklės. Jei tolesnė taisyklė rasta, ji iškeliama ir toliau tikrinama taisyklių bazėje. Dauguma taisyklėmis paremtų sistemų leidžia vartotojui pasirinkti konfliktų sprendimo strategiją, kuri naudojama, kai reikia iškelti taisykles tam tikra tvarka, jei yra daugiau nei viena taisyklė, tenkinanti sąlygas.

Atgalinės grandinės metodas. Dirbant atgalinės grandinės metodu pradedama nuo tikslo ir ieškoma žinių bazėje jį patvirtinančių taisyklių, kurių tikslai sutampa. Radus tokią taisyklę jos sudėtinė sąlyga iškeliama kaip tikslas, ir vėl sukasi ta pačia tikrinimo grandine. Kai visos taisyklės patvirtintos, gaunamas rezultatas. Jei bent viena iš sąlygų nepatvirtinta ir nebėra tikrinimui reikalingų kitų sutampančių taisyklių, išeinama neradus sprendimo.

Kai kurios ekspertinės sistemos, naudodamos atgalinės grandinės taisykles, naudoja rezultato gavimo išsaugojimą duomenų bazėje tam, kad situacijai pasikartojus būtų galima lengviau rasti sprendimą.

12 lentelė. Sprendimo paieškos strategijų palyginimas

Tiesioginės grandinės metodas	Atgalinės grandinė metodas
Planavimas, kontrolė.	Diagnozė.
Data-driven metodas.	*Goal-driven* metodas.
Naudojama iš apačios į viršų sprendimo paieškos strategija.	Naudojama iš viršaus į apačią sprendimo paieškos strategija.
Randa galimą išvadą pagal duotus faktus.	Randa faktus, kurie atitinka pateiktą hipotezę.
Surenka visus duomenis, tam turi pateikia visus klausimus vartotojui.	Dažnai veikia greičiau, nes išvengia nereikalingų klausimų.
Naudinga naudoti kai reikia surinkti visą informaciją iš vartotojų.	Naudinga naudoti, kai taisyklės talpina daug rezultatų. Privalo būti naudojamas, kai žinių bazė talpina begalinį skaičių galimų faktų.

1.8.3. Neapibrėžtumų valdymo metodai

Labai mažai yra realių problemų, kurių galimas sprendimas laikomas neabejotinai teisingu, arba faktai ne visada būna visiškai teisingi. Dažnai tenka tirti problemas, kurios sudarytos iš abejotinų sąlygų. Tokias problemas labai sunku valdyti, taigi žiniomis pagrįstos sistemos projektuotojas turi atidžiai pasverti nenaudingus kompromisus ir pritaikyti konkrečiai situacijai, bei pasirinkti būdą neapibrėžtumo valdymui. Išanalizavau 4 būdus, galimus naudoti neapibrėžtumo valdymui [10]:

- Tikimybių teorija
- Pasitikėjimo faktoriai
- Dempster-Shafer teorija
- Galimybių teorija

Tikimybių teorija. Yra trys mokymai, kurių kiekvienas naudoja panašius matematinius metodus. Vienas dažniausiai naudojamas žiniomis paremtose sistemose yra Bayesian (žiniomis paremtas) metodas [10].

Pasitikėjimo faktoriai (kartais vadinami Stenford Certainty Factors). Pasitikėjimo faktoriai naudojami išreikšti žinių tikslumui [10]. Tai nėra tikimybė, šis skaičius atspindi bendrą hipotezės pasitikėjimą turima informacija. Jis taikomas faktams, taisyklėms ir išvadoms. Sprendimas yra grindžiamas įrodymais arba įrodymų interpretacija ir yra subjektyvus.

Dempster-Shafer teorija. Tai matematinė įrodymų teorija, kuri gali būti interpretuojama kaip tikimybių teorijos generalizacija, kur tikimybės yra priskiriamos rinkiniams [10]. Tradicinėje tikimybių teorijoje faktai yra siejami tik su vienu teisingu įvykiu. DST teorijoje, faktai gali būti siejami su daugeliu galimų įvykių, pvz. įvykių rinkiniu.

Galimybių teorija. Galimybių teorija yra matematinė teorija, skirta vertinti tam tikrų rūšių neapibrėžtumams, ir yra laikoma tikimybių teorijos alternatyva. Ji yra neraiškių aibių ir neraiškios logikos praplėtimas [14]. Galimybių teorija nustato kokio tikslumo laipsnį turi turėti įvykis, kad jis būtų įmanomas ir kokiu tikslumu mes esam tikri dėl jo atsitikimo, kai nėra žinoma jo atsitikimo vertė [10].

Lentelė Nr. 1. Neapibrėžtumų valdymo metodų palyginimas

Neapibrėžtumo valdymo metodas	Privalumai	Trūkumai
Tikimybių teorija ir Bajeso taisyklė	• Egzistuoja formalūs aprašai; • Gerai apibrėžta semantika spendimų priėmimui; • Atspindi tikrovę (aposterioriniai); • Naudojanti Bajeso taisykle žinios atvaizduojamos kaip ankstesnių tikimybių rinkinys sulyginamas su duomenų sąlyginėmis tikimybėmis; • Naudojant Bajeso klasifikaciją sprendimų priėmimas vykdomas palyginti greitai.	• Naudoja didelį kiekį duomenų; • Gali būti netikslu naudojant subjektyvias tikimybes; • Tikimybė turi būti priskirta net ir tada, kai nėra jokios informacijos; • Reikalauja įvertinti visus turimas žinias; • Sudėtingi sakiniai su sąlyginėmis priklausomybėmis negali būti išskaidytos į atskiras nepriklausomas dalis; • Visada reikalaujama priorinės tikimybės, kurią yra sunku apibrėžti.
Pasitikėjimo faktoriai	• Neapibrėžtumas faktuose ir išvadose ir taisyklėse; • Patogu naudoti, kai tikimybės nėra žinomos, arba jas sunku apibrėžti.	• Kai kuriais atvejais rezultatai gali priklausyti nuo tvarkos, kuria faktai yra aprašomi.; • Nepriklausomų faktų kombinacija yra visada nesėkminga; • Naujos žinios gali keisti jau egzistuojančių žinių pasitikėjimo faktorius; • Netinkamas ilgoms grandinėms.
Dempster-Shafer teorija	• Egzistuoja aiškūs ir griežti aprašymai; • Metodas koncentruojasi ne į vieną išvadą, o į kelias kombinacijas;	• Nėra galimybės atpažinti dažniausiai pasitaikančių tikimybių; • Reikalauja didelių ir sudėtingų skaičiavimų.

	• Visų galimų išvadų rinkinys yra paskirstomas į kelias kombinacijas.	
Galimybių teorija ir neraiškių aibių teorija	• Nereikalauja matematinio proceso modelio.	• Nėra aiškios metodikos, kaip pateikti turimas žinias ir patirtį.

1.9. Išvados

Visame informacijos saugos audito procese daugiausiai kompetencijos ir žinių reikalauja duomenų analizės ir duomenų įvertinimo etapai. Informacijos saugos auditorius, vykdydamas auditą, turi turėti atitinkamas priemones, gebėjimus, metodus ir praktiką. Iš auditoriaus reikalaujama ir gerų analitinių sugebėjimų duomenų analizei atlikti bei plačios apimties informacinių technologijų žinių, tiek iš techninės, tiek iš programinės, tiek iš valdymo srities. Todėl svarbus uždavinys yra palengvinti auditoriaus darbą, pasinaudojant automatizuotomis priemonėmis.

Lietuvos pripažintu dažniausiai naudojamu standartu yra LST ISO/IEC 27001:2006 geros praktikos standartas, pagal kurį priima saugumo atitikties vertinimo metodika. Jis naudojamas siekiant ISMS sertifikavimo. Tačiau mažos ir vidutinės įmonės, bei dalis viešųjų įstaigų iš viso neatlieka informacijos saugos audito dėl procedūros sudėtingumo, lėšų trūkumo bei operuojamos informacijos svarbos nuvertinimo.

Analizuotos programos, skirtos informacijos saugos auditui, pasižymi savo paprastumu, tačiau jos yra brangios. Be to jos labai ribotos savo funkcinėmis galimybėmis, dėl ko dalį darbo, kurio jos neaprėpia, reikia atlikti, kam auditoriaus žinių gali nepakakti. Pvz.: atlikus auditą ir nustačius saugos spragas organizacijoje reikia paruošti veiksmų įgyvendinimo planą saugai pagerinti. Jei naudojama auditui automatizuota sistema nepateikia rekomendacijų spragoms ištaisyti, tuomet prireiks eksperto, kurie padės sudaryti planą ir parinkti saugos priemones. Tuo tarpu egzistuoja universalios rizikų vertinimo sistemos, tokios kaip RiskWatch arba Buddy System, kurios pasižymi savo funkcionalumu. Taip pat nei viena sistema nepalaiko lietuvybės bei yra diegiamos į vartotojo kompiuterį kas nėra patogu. Lietuviškų analogiškų produktų surasti nepavyko.

Taip pat išnagrinėti žiniomis paremtų naudojamų sistemų realizavimo metodai: ekspertinės sistemos, sprendimų pramos sistemos ir dirbtiniai neuroniniai tinklai. Visi metodai pasižymi žmogaus minčių modeliavimu. Geresnių rezultatų galima pasiekti jungiant sprendimų

paramos sistemas su ekspertinėmis sistemomis. Tokiu atveju ekspertinė sistema, pasinaudojama savo sprendimo paieškos galimybėmis pateikia detalesnes rekomendacijas.

2. INFORMACIJOS SAUGOS AUDITO SPRENDIMŲ PARAMOS SISTEMOS MODELIS

2.1. Tikslai

Pagrindinis tikslas yra sukurti informacijos saugos audito sprendimų paramos sistemą, skirtą informacijos saugos auditui atlikti auditoriui neprofesionalui mažose ir vidutinėse įmonėse, bei pateikti sprendimus informacijos saugai organizacijoje gerinti.

Sistema vartotojams turi pateikti klausimus, ir pagal vartotojo atsakymus išduoti informacijos saugos organizacijoje įvertinimą bei rekomendacijas saugai gerinti. Sistema turi gebėti vertinti rizikas kurios neturi aiškiai apibrėžtų reikšmių.

2.2. Reikalavimų specifikavimas

Tikslinės vartotojų grupės.

Informacijos saugos auditorius neprofesionalas. Sistema bus skirta organizacijos darbuotojams, atsakingiems už informacijos saugą organizacijoje bei visam vadovaujančiam personalui, neturinčiam specifinių techninių saugos arba audito procedūros žinių, bet galintiems prieiti prie svarbios informacijos. Jie galės atlikti vidinį informacijos saugos auditą organizacijoje.

Informacijos saugos ekspertas. Kadangi sistema turi leisti plėsti klausimų bei taisyklių bazę, tai ji turi būti skirta taip pat ir darbuotojams, turintiems techninių žinių, t.y. kompiuterių tinklų inžinieriams, aukštesniosios grandies sistemų administratoriams.

Reikalavimai sprendimo pateikimui.

Sistema turi pagal vartotojų įvestas žinias pateikti esamą organizacijos informacijos saugos situaciją identifikuojant nesaugias sritis, bei pateikti rekomendacijas saugos spragoms užtaisyti. Taip pat turi būti galimybė kaupti ir saugoti atlikto audito duomenis.

Sistemos diegimo aplinka.

Sistemos įdiegti į kiekvieną kompiuterį nereikia. Jis bus pasiekiamas iš bet kurios interneto ryšį turinčios darbo vietos, kurioje nėra draudžiama naudotis Java Server Pages (CGI), Active Server Pages (ASP), Common Gateway Interface (SGI).

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)

Sistemos funkciniai reikalavimai

Sistema informacijos saugos auditoriui neprofesionalui turi:

- leisi įvesti informaciją, kurios sistema prašo;
- pateikti identifikuotų saugumo spragų sąrašą ir rekomendacijas;
- leisti spausdinti atliktas inforamcijos saugos rizikų ataskaitas.

Sistema informacijos saugos ekspertui turi:

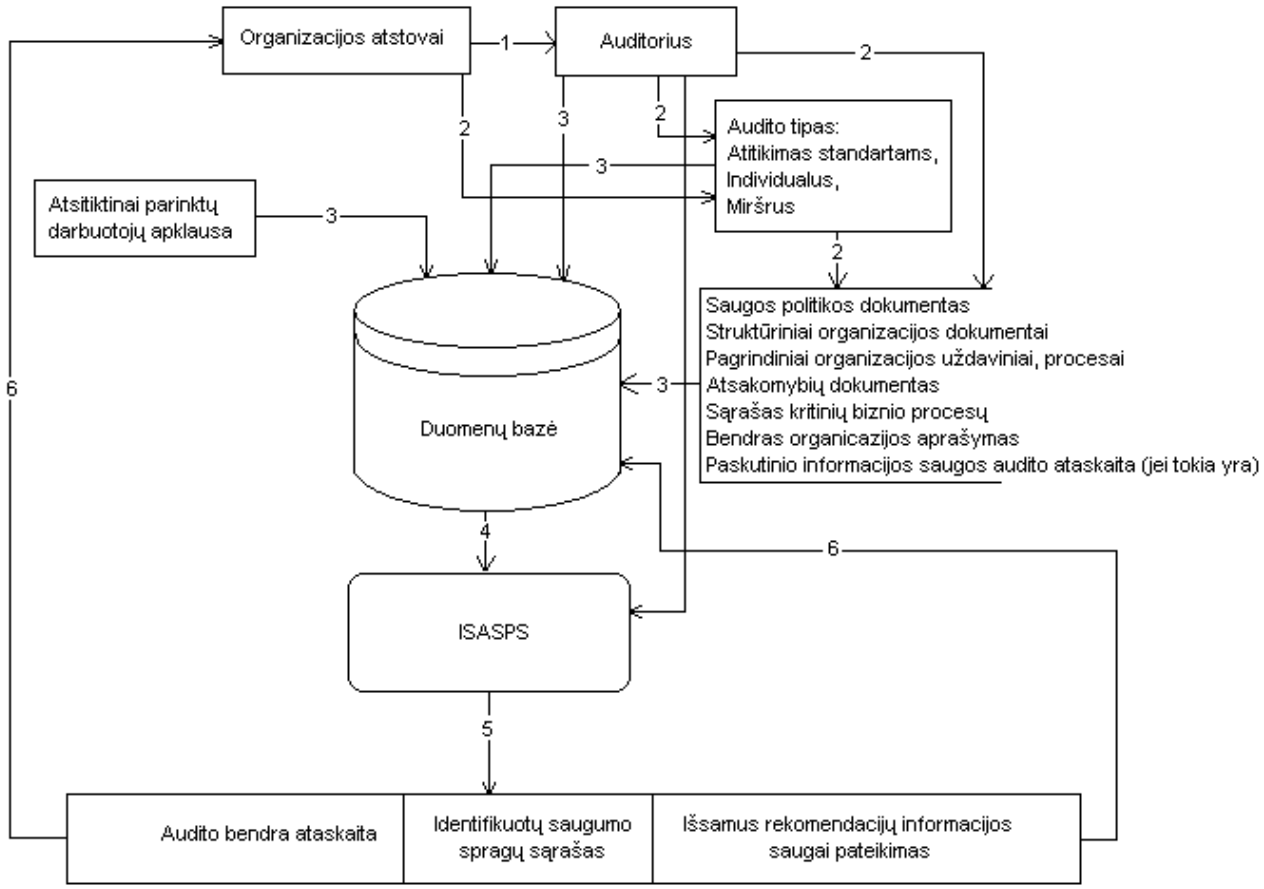
- leisti nesudėtingai keisti ir pildyti žinių bazę: kurti taisykles, klausimus, rekomendacijas;

Sistemos nefunkciniai reikalavimai

- Lengvai suvokiama vartotojo sąsaja;
- Klausimai apibrėžti taip, kad vartotojui būtų suprantami kuo aiškiau;
- Sistema turi būti sukurta taip, kad informacijos saugos auditoriumi galėtų būti bet kuris organizacijos darbuotojas, t.y. informacijos saugos auditui atlikti neturi būti reikalingas profesionalus auditorius;
- Klausimai paruošti atsižvelgiant į nacionalinį inforamcijos saugos standartą LST ISO/IEC 27001:2006.

2.3. Informacijos saugos audito procesas dalyvaujant automatizuotai priemonei

Informacijos saugos audito procesas dalyvaujant ISASPS pavaizduotas paveiksle:



7 pav. Informacijos saugos audito procesas dalyvaujant IS audito sistemai

Čia apibrėžiami 6 informacijos saugos audito etapai:

- 1 etapas. Audito inicializavimas. Kai auditorius ar jų grupė susitinka su audituojamos organizacijos atstovais, kurie paskirti atsakingi už savo organizacijoje vykdomą informacijos saugos auditą.
- 2 etapas. Abiems šalims (tiek auditoriui, tiek organizacijai) sutarus parenkamas audito tipas. Ar bus vykdomas atitikimo standartams auditas, ar individualus, nuo to priklausys ir informacijos parinkimas auditui.
- 3 etapas. Informacijos surinkimas ir patalpinamas duomenų bazėje. Tai visa reikalinga informacija informacijos saugos auditui atlikti, įskaitant saugos dokumentus, organizacijos struktūrą, informacijos saugos politiką ir kt.
- 4 etapas. Naudojantis automatizuota informacijos saugos audito sprendimų paramos sistema (ISASPS) vykdoma informacijos saugos organizacijoje analizė. Analizės metu atliekami 2 veiksmai:
    - ištiriami apsibrėžti informacijos saugos aspektai, ieškant saugumo spragų. Vykdant individualų auditą sritys parenkamos auditoriaus, derinant su

organizacijos vadovybe išskiriant rizikingiausias. Jei auditas vykdomas siekiant standarto ISO 27001, tuomet analizuojama 11 saugumo sričių, apibrėžiamų standarte:

- Saugumo politika
- Saugos organizavimas
- Išteklių valdymas
- Personalo sauga
- Fizinė ir aplinkos sauga
- Komunikacijų ir operacijų valdymas
- Prieigos kontrolė
- Informacinių sistemų įsigijimas, kūrimas ir priežiūra
- Informacijos saugos incidentų valdymas
- Veiklos tęstinumo valdymas
- Sistemos atitikimas reikalavimas

  - Pateikiamas išsamus sprendimas identifikuotoms informacijos saugos spragoms užtaisyti. Sprendimų tikslumui užtikrinti naudojamos neraiškios logikos metodai. Saugos spragos pateikiamos prioriteto jų ištaisymui tvarka: nuo labiausiai keliančios grėsmę iki mažiausiai keliančios grėsmę, kartu pateikiant ir išsamią rekomendaciją saugos didinimui.

- 5 etapas. ISASPS rezultatų pateikimas. Pateikiamas identifikuotų spragų sąrašas ir priemonė (sprendimai) informacijos saugai pagerinti.
- 6 etapas. Audito ataskaita yra pateikiama audituojamos organizacijos atstovams bei vykdant grįžtamą ryšį papildoma duomenų bazė duomenimis, gautais audito metu, kurie bus naudojami vėlesniems auditams atlikti.

2.4. Sistemos architektūra

Atsižvelgiant į informacijos saugos audito procesą buvo sumodeliuota intelektualios sprendimų paramos sistemos struktūrą, kuri pateikiama pav. 8.

Čia realizuoti visi tipiniai sprendimų paramos sistemos komponentai: žinių bazė, išvadų generatorius, užklausų apdorojimo posistemė ir grafinė vartotojo sąsaja. Apibrėžti du sistemos vartotojai: inforamcijos saugos auditorius ir žinių inžinierius. Kurie dirba su sistema per grafinę vartotojo sąsają. Žinių inžinierius dirba per savo specialią žinių bazės kūrimo aplinką pildo

žinias, kurios po to per patalpinamos tiesiai į žinių bazę. Čia žinių inžinierius gali kurti naujos iškeltos problemos modelį ar jį koreguoti. Tuo tarpu auditorius naudojasi jau sukurtais modeliais ir per užklausų apdorojimo posistemę siunčia užklausas į sistemą, gauna atvaizduotus rezultatus, gali pasinaudoti sistemos pagalbos galimybe ir sužinoti, kodėl yra klausiami atitinkami klausimai siekant spręsti problemai.

Išvadų generatorius vaidina pagrindinį vaidmenį. Jis atlieka dvi pagrindines funkcijas – išvadų generavimas ir kontrolė. Jis priima komandas, persiųstas iš užklausos ir veiksmo dalis, kuriuos siunčia vartotojas per užklausų ir apdorojimų posistemės, vykdo gautas komandas, kontroliuoja priėjimą prie duomenų bazės ir žinių bazės, vykdo modelius, nuskaito žinias iš žinių bazės ir daro išvadas. Problemų procesorius turi du pagrindinius išvesties mechanizmus: (1) projektavimo ir vedimo į problemos sprendimą ir (2) atitinkamo modelio ir naudojamos programos vykdymo kontrolės. Naudojama programa yra naudojama sprendimo procese duomenų struktūros konvertavime, specialių duomenų atvaizdavime.

Po problemos modelio sukūrimo per modeliavimo posistemę yra pateikiama išvadų generatoriui. Pirmas išvadų generatoriaus mechanizmo darbas yra nurodyti sprendimo strategiją, paremtą problemos modeliu ir išvesti sprendimo procesą, kuris ves į problemos sprendimą. Proceso metu antras mechanizmas bus aktyvuotas iškviečiant duomenų bazę ir priskiriant parametrų reikšmes. Antras mechanizmas taip pat kontroliuoja atitinkamos naudojamos programos parinkimui, nustato modelių ir naudojamų programų tvarkaraštį ir užtikrina, kad jos atliekamos nurodyta tvarka.

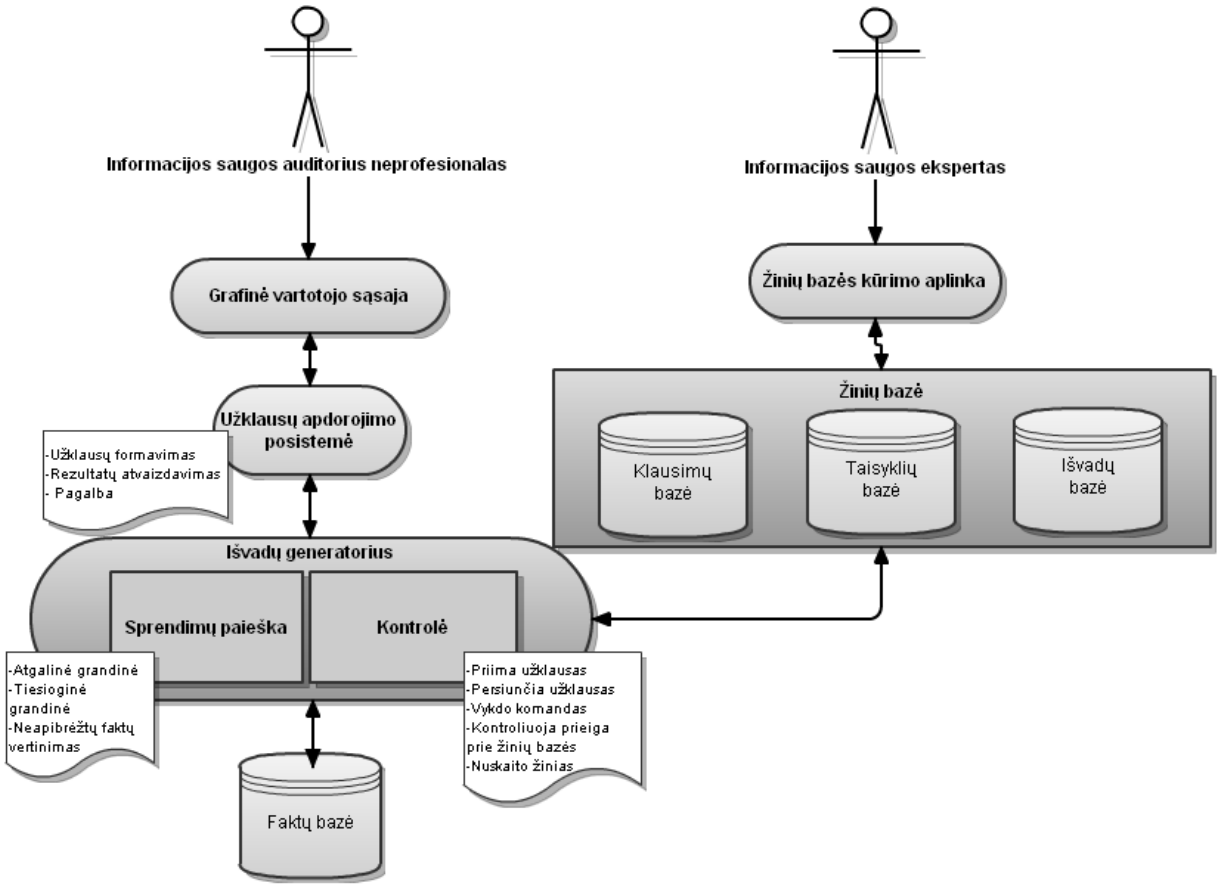
Informacijos saugos sprendimų paieška apibrėžiama tam tikrais sprendimų metodais, t.y. pasitikėjimo faktoriais ir jų vertinimu tikimybinėmis funkcijomis. Kontrolės procesas priima siunčiamas užklausas į žinių bazę ir iš jos, vykdo nurodytas komandas.

Žinių bazė sudaryta iš:

- Klausimų bazės – aprašo klausimų bazę, kuri yra pateikiama auditoriui testo atlikimo metu;
- Taisyklių bazės – aprašo eksperto žinias (heuristinis metodas) Jei-Tai forma, modeliuoja žmogaus mąstysena, aprašo duotos situacijos veiksmą;
- Išvadų bazės – aprašo galimas išvadas, kurios pateikiamos auditoriui auditavimo proceso pabaigoje.

Faktų bazė aprašo žinias apie žinomą problemą, sudaryta iš atributų ir jų reikšmių, kurias vartotojas įveda atlikdamas testą. Faktų bazėje taip pat saugomi senesnių auditų rezultatai tokia

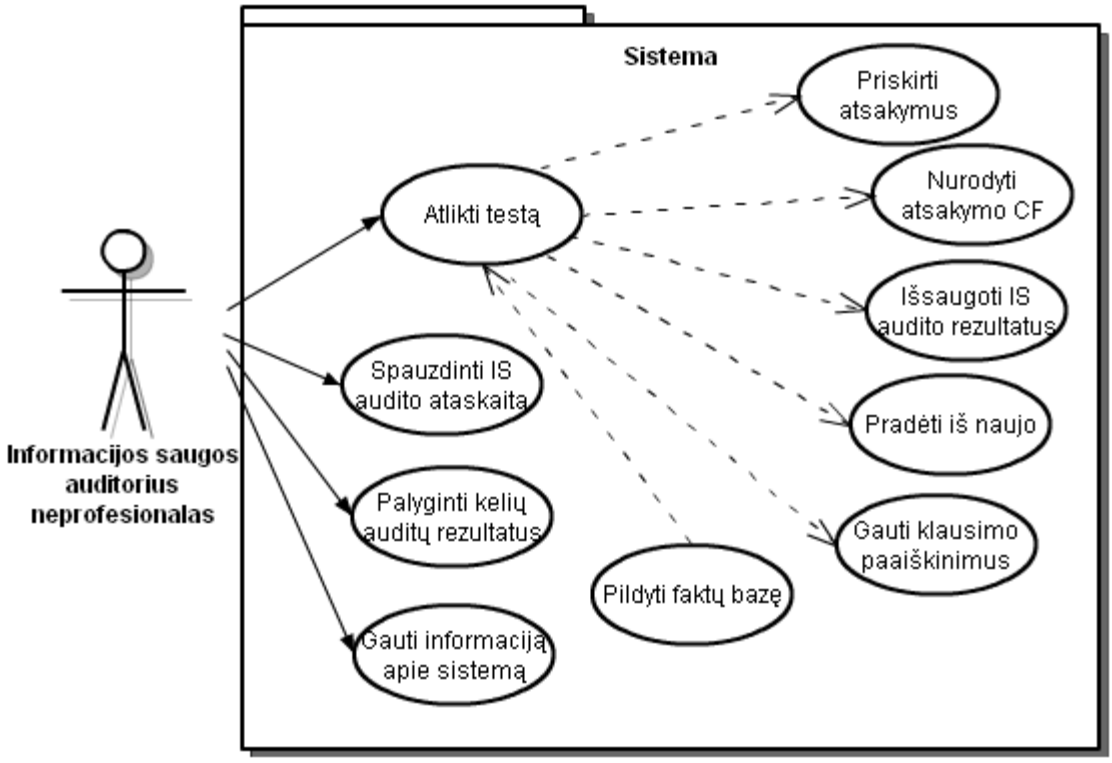
pat forma,t.y. atributų ir jų reikšmių, bei išvadų. Išvadų generatorius pildo, keičia ir vertina faktus žinių bazėje.



8 pav. Siūlomos sprendimų paramos sistemos architektūra

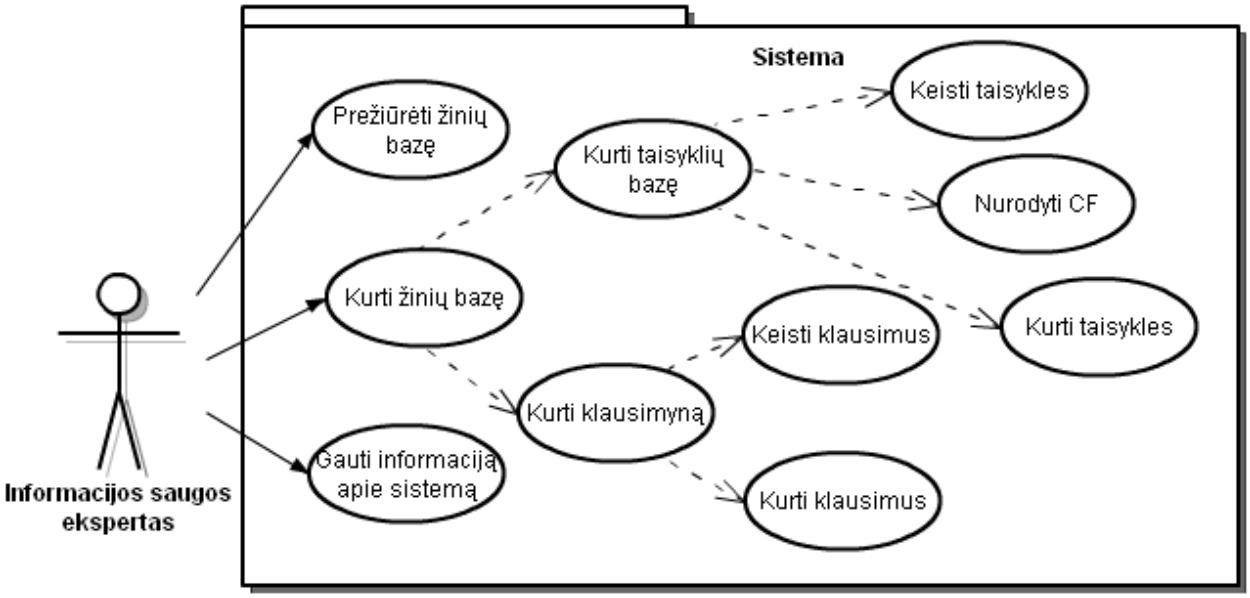
2.5. Panaudojimo atvejų diagramos

Informacijos saugos audito sprendimo paramos sistemoje galimos dvi vartotojo rolės: informacijos saugos auditorius neprofesionalas ir informacijos saugos ekspertas.



9 pav. Informacijos saugos auditoriaus neprofesionalo panaudojimo atvejų diagrama

Informacijos saugos auditorius, tai tas organizacijos darbuotojas, kuris yra atsakingas už informacijos saugą organizacijoje ir/arba vadovauja personalui, neturintis specifinių techninių saugos žinių, bet galintis prieiti prie svarbios informacijos. Jis atlieka auditą su jau paruošta žinių baze. Auditorius atidaro žinių bazę ir iš sudaryto klausimyno jam pateikiamas klausimas. Jis įveda norimus duomenis, nurodo savo atsakymo pasitikėjimo lygį procentais. Prireikus suteikiama galimybė pateikti auditoriui klausimo paaiškinimą, t.y. kokia taisyklė yra tikrinama. Vartotojas suvedęs visus prašomus duomenis gauna saugos spragų sąrašą, rekomendacijų saugai pagerinti sąrašą lentelės forma. Taip pat, auditoriui suteikiama galimybė atspauzdinti rezultatus, bei juo išsaugoti. Informacijos saugos auditorius taip pat gali palyginti dviejų pasirinktų auditų rezultatus.



10 pav. Informacijos saugos eksperto panaudojimo atvejų diagrama

Informacijos saugos ekspertas yra tas žmogus, kuris ruošia žinių bazę auditoriui. Jis esant reikalui gali koreguoti jau įvestas taisyklės, jas papildyti, taip pat koreguoti ir įvesti naujus faktus ir klausimus. Labai svarbu teisingai nurodyti pasitikėjimo faktorius, nes jais remiantis vertinami galimi problemų sprendimai.

2.6. Žinių ir duomenų bazių struktūra

Tikslas taisyklėmis paremtose sistemose yra kaupti JEI-TAI taisykles iš žmonių ekspertų arba bazių, talpinančių pradines žinias. Žinių bazė ir išvadų generatorius yra naudojami reikalingų išvadas taikymui iš taisyklių ir faktų, pateiktų vartotojui.

Taisyklėmis paremtas modelis aprašomas taip [34]:

$R = \langle U, A, D, F \rangle$

Kur $U = \{U_i; i = 1,...,T\}$ yra rinkinys pradinių atributų (faktų), kurių kievienas turi savo reikšmę iš galutinio masyvo rinkinio $A = \{A_1, A_2,..., A_T\}$. $A = \{A_{ij}; j = 1,..., J_i = |A_i|\}$ yra rinkinys reikšmių ar pasiūlymų atributams $U = \{U_i; i = 1,...,T\}$. Masyvas $\{U_i, U_2,..., U_T\}$ apibrėžia sąrašą baigtinių salygų, kurios aprašo pirminę problemos būseną, kurios gali būti jungiamos loginėmis operacijomis "$\wedge$", "$\vee$". "$\wedge$" yra loginė jungimo operacija, atitinkanti veiksmą "*IR*", o "$\vee$" – loginė jungimo operacija atitinkanti veiksmą "*ARBA*". $D = \{D_n; n = 1,..., N\}$ yra rinkinys visų padarinių, kurios gali būti išvados arba veiksmai. *F* yra loginė funkcija, atspindinti santyki tarp sąlygų ir su jomis susijusių išvadų.

Tam, kad sukurti taisyklių bazę, pirmiausia nustatoma, kuris rinkinys kuriam atributui turi būti naudojamas ir kaip daug reikšmių turi būti naudojama. *K*-toji taisyklė taisyklių bazėje aprašytoje sujungimais „jei-tai“ gali būti aprašyta taip [34]:

$$R_k : jei\ A_1^k \wedge A_2^k \wedge ... \wedge A_{T_k}^k, tai\ D_k$$

Kur $A_i^k (i = 1,...,T_k)$ yra nurodyta vertė *i*-tojo anksčiau įvykusio *k*-toje taisyklėje. $D_k (\in D)$ yra pasėkmė *k*-toje taisyklėje.

2.6.1. Bendri žinių aprašymo parametrai

1) ***Atributų svoris***. Taisyklėmis paremtose sistemose svarbus yra atributų svoris. Pvz.: informacijos saugoje tam tikrų faktų kombinacija identifikuoja saugumo spragą. Svarbu priskirti svorį kiekvienam faktui (atributui), kad surasti spragą.
2) ***Taisyklių svoris***. Svoris gali taip pat būtų priskirtas taisyklei, kuri yra naudojama nurodyti taisyklės svarbai tam tikrai išvadai.
3) ***Atsakymo pasitikėjimo svoris***. Svoris taip pat gali būti priskirtas atsakymui, t.y. informacijos saugos auditorius, atlikdamas auditą ir atsakydamas į klausimus gali nurodyti savo atsakymo užtikrintumo laipsnį procentais.
4) ***Bendras minimalus pasitikėjimo svoris***. Tai svoris, priskiriamas žinių bazei, pagal kurį sprendžiama, ar pateikti išvadas vartotojui kaip informacijos saugos audito rezultatą. Jei išvados pasitikėjimo svoris yra mažesnis už nurodytą minimalų pasitikėjimo svorį, tuomet laikoma, jok neužtenka pasitikėjimo, kad išvada būtų pateikta auditoriui.

Taisyklių, atributų ir bendras minimalus pasitikėjimo svoris yra priskiriami žinių įgijimo fazėje, kai taisyklių bazė yra kuriama. O atsakymo pasitikėjimo svoris priskiriamas audito metu.

2.6.2. Taisyklių bazės struktūra

Nurodant skaičiavimams pasitikėjimo laipsnį, atributų svorius ir taisyklių svorius taisyklėse, *k*-toji taisyklė yra išplečiama:

$$R_k : jei\ A_1^k \wedge A_2^k \wedge ... \wedge A_{T_k}^k, tai\ D_k \quad (1)$$

Su pasitikėjimo laipsniu $\overline{\beta}_k$, taisyklės svoriu θ_k ir atributų svoriais $\delta_{k1}, \delta_{k2}, ..., \delta_{kT_k}$, kur $A_i^k (i = 1,...,T_k)$ yra *i*-tojo atributo reikšmė *k*-toje taisyklėje, T_k yra atributų skaičius, naudojamų

k-toje taisyklėje, ir $\overline{\beta}_k$ yra pasitikėjimo laipsnis, kuriam $D_k (\in D)$ yra įtikinamas, kad būtų tiesa, duotai $A_1^k \wedge A_2^k \wedge ... \wedge A_{T_k}^k$ *k*-toje taisyklėje. θ_k yra susijęs svoris *k*-tosios taisyklės, ir $\delta_{k1}, \delta_{k2}, ..., \delta_{kT_k}$ yra susiję svoriai T_k atributų, naudojamų *k*-toje taisyklėje.

Taisyklė (1) gali būti toliau taikoma kaip pagrindinė taisyklė, naudojant pasitikėjimo struktūrą, kur visos galimos pasekmės yra asocijuotos su pasitikėjimo laipsniu. Rinkinys pagrindinių taisyklių tęsia taisyklių bazę su pasitikėjimo struktūra (vadinama pasitikėjimo taisyklių baze) kaip [34]:

R_k : *jei* $A_1^k \wedge A_2^k \wedge ... \wedge A_{T_k}^k$, *tai*

$\{(D_1, \overline{\beta}_{1k}), (D_2, \overline{\beta}_{2k}), ..., (D_N, \overline{\beta}_{Nk})\}$

$(\sum_{i=1}^{N} \overline{\beta}_{ik} \leq 1)$, su taisyklės svoriu θ_k ir atributo svoriais $\delta_{k1}, \delta_{k2}, ..., \delta_{kT_k}$ $k \in \{1, ..., L\}$

Kur $\overline{\beta}_{ik} (i \in \{1, ..., N)$ yra pasitikėjimo laipsnis, kuriam D_i yra įtikimas, kad būtų pasėkmė salygos "*jei*", *k*-tojoje taisyklėje, įvedimas tenkina paketo atributus $A^k = \{A_1^k, A_2^k, ..., A_{T_k}^k\}$. *L* yra skaičius visų taisyklių taisyklių bazėje. Jei $\sum_{i=1}^{N} \overline{\beta}_{ik} = 1$, *k*-toji paketo taisyklė laikoma pilna. Jei $\sum_{i=1}^{N} \overline{\beta}_{ik} = 0$, tai laikoma, kad visiškai ignoruojama išvada, duotiems imputams *k*-tojoje paketinėje taisyklėje.

Pvz.:

R_k : *jei* "nesėkmių rodiklis yra dažnas" *ir*
"padarinių sunkumas yra kritinis" *ir*
"nesėkmės tikimybė yra mažai tikėtina",
tai "saugumo lygis yra"
{(geras,0},(vidutinis, 0),(patenkinamas, 0.7), (silpnas, 0.3)}

Kur {(geras,0},(vidutinis, 0),(patenkinamas, 0.7), (silpnas, 0.3)} yra tikėtinumo pasiskirstymas išvadoje, teigiant, jok 70% tikėtina, kad saugos lygis yra patenkinamas ir 30% tikimybė, kad saugos lygis yra silpnas. Šioje tikėjimo taisyklėje bendras pasitikėjimo laipsnis yra 0.3+0.7=1, taigi, vertinimas yra pilnas. Orientacinių verčių rinkinys neteisingam matavimui yra A_{FR} ={labai žemas, žemas, ginčytinai žemas, vidutinis, ginčytinai įprastas, įprastas, ir aukštai įprastas}.

2.7. Žinių aprašymas sistemoje

Sistemoje žinioms aprašyti yra išskirtos trys bazės: išvadų bazė, klausimų bazė ir taisyklių bazė. Žinioms bazėje aprašyti naudosiu Bekaus – Nauro forma (BNF).

2.7.1. Išvadų bazė

Išvadų bazė, tai sąrašas visų informacijos saugos audito sistemos galimų išvadų. Išvadų bazę sudaro:

- galimos galutinės išvados (<išvada>), kurios išplaukia iš taisyklių, kaip rezultatai (<taisyklės išvada>);
- standartinė išvada, t.y. išvada pagal nutylėjimą (<pagal nutylėjimą>), kuri naudojama, kai vartotojo gauti faktai neatitinka nei vienos taisyklės;
- minimalus pasitikėjimo faktorius (<minimalus pasitikėjimas>), kuris vertinamas renkant reikiamą išvadą. Jei minimalus pasitikėjimo faktorius bus didesnis nei kad gautas išvados pasitikėjimo faktorius, tuomet tokia išvada bus nerodoma;
- išvados variantų skaičius (<variantų skaičius>) yra skaičius, kuris nurodo kiek tokios pat išvados yra galimų skirtingų reikšmių

Žinias bazėje aprašysime naudojantis Bekaus – Nauro forma (BNF):

```
<išvadų bazė>                ::=<išvada> {,<išvada>}
                             <pagal nutylėjimą>
                             <minimalus pasitikėjimas>
                             <variantų skaičius>
<išvada>                     ::=<sritis>: <rekomendacija>
<pagal nutylėjimą>           ::=<raidė>[{<raidė>|<skaitmuo>}]
<minimalus pasitikėjimas>    ::=(@)<skaičius>
<variantų skaičius>          ::=<taisyklės išvada>:=<skaitmuo>
<sritis>                     ::=([)<raidė>(])[{<raidė>|<skaičius>}]
<rekomendacija>              ::=(“)<raidė>(”)[{<raidė>|<skaičius>}]
<skaičius>                   ::=<skaitmuo> {<skaitmuo>}
<raidė>                      ::= a | ą | b | c | d | e | ę | ė | f | g | h |
                             i | į | y| j | k | l | m | n | o | p | q | r | s
                             | š | t | u | ų | ū | v | w | x | z | ž
<skaitmuo>                   ::= 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
<skirtukas>                  ::= ?
```

2.7.2. Taisyklių bazė

Taisyklės, tai žinių forma, kuria žinios aprašomos žinių bazėje. Žinių bazę sudaro:

- JEI-TAI taisyklės (<taisyklė>)
- Taisyklės susideda iš sąlygų dalies (<sąlyga>) ir išvadų dalies (<išvada>)
- Taisyklės tiek sąlygos ir išvadų dalys gali būti sudurtinės, t.y. apjungtos IR, ARBA operacijomis
- Sąlygos (<sąlyga>) sudarytos iš atributų (<atributas>) ir jų reikšmių (<reikšmė>)
- Išvados sudarytos iš srities (<sritis>) ir rekomendacijos (<rekomendacija>) tai sričiai
- Taisyklės jokių loginių jungčių viena su kita neturi, t.y. jos viena nuo kitos nepriklausomos
- Atributas (<atributas>) ir jo reikšmė (<reikšmė>) yra faktai, kurie gaunami iš vartotojo atsakant į klausimus. Kiekvienas atributas turi savo susijusias reikšmes
- Pasitikėjimas (<pasitikėjimas>) žymimas skaičiumi tarp 0 ir 100 prieš tai pridedant simbolį „%“.
- Pasitikėjimo faktorius (svorinius koeficientus) gali turėti:
    - Taisyklės sąlygos
    - Taisyklės išvados
    - Jei taisyklės yra jungtinės, tai kiekviena taisyklės sąlygos dalis ar išvados dalis gali turėti savo svorinius koeficientus

Žinias bazėje aprašysime naudojantis Bekaus – Nauro forma (BNF):

```
<taisyklių bazė>  ::=<taisyklė> {,<taisyklė>)
<taisyklė>        ::= JEI <sąlyga> TAI <išvada>
<sąlyga>          ::=  <atributas>  <operatorius>  <reikšmė>  [<pasitikėjimas>]
                  {[<operacija>]      [<atributas>   <operatorius>   <reikšmė>
                  <pasitikėjimas>]}
<išvada>          ::= <sritis>: <rekomendacija> [<pasitikėjimas>]
                  {[<operacija>] [<sritis>: <rekomendacija> <pasitikėjimas>]}
<pasitikėjimas>   ::= (@)<skaičius>
<atributas>       ::= ([)<raidė><skirtukas>(]) {raidė|skaitmuo }
<reikšmė>         ::= (“)<raidė>(”) {raidė|skaitmuo }
<operacija>       ::= IR | ARBA | NE
<skaičius>        ::= <skaitmuo> {<skaitmuo>}
```

```
<raidė>           ::= a | ą | b | c | d | e | ę | ė | f | g | h | i | į | y| j
| k | l | m | n | o | p | q | r | s | š | t | u | ų | ū | v | w | x | z | ž
<skaitmuo>        ::= 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
<operatorius>     ::= = | < | > | ! | :
<skirtukas>       ::= ?
```

2.7.3. Klausimų bazė

Klausimų bazė, tai sistemos vartotojui pateikiamų klausimų sąrašas su galimais variantais atsakymų. Klausimą sudaro:

- Atributas (<atributas>), kurio reikšmę reikia identifikuoti
- Klausimo lauko tipas (<lauko tipas>), t.y. koks lauko tipas bus naudojamas vartotojo sąsajai pateikti klausimui. Galimi 4 laukų tipai:
    - TaipNe – galimi pasirinkimo variantai: taip, ne
    - Multi – su galimybe pažymėti kelis atsakymo variantus iš pateiktų
    - Multi2 – su galimybe pažymėti kelis atsakymo variantus iš pateiktų, papildomai automatiškai pasiūlant variantą „Nežinau atsakymo“
    - Pasirinkti – galimybė pasirinkti vieną atsakymą iš pateikto sąrašo
    - Skaičius – galimybė įvesti skaitinį reikšmę
- CF – funkcijos aktyvavimo operacija (<operacija>), leidžianti vartotojui priskirti savo atsakymo pasitikėjimo laipsnį. Tai nėra būtinas laukas
- Klausimo tekstas (<klausimo tekstas>)
- Klausimo galimos reikšmės (<reikšmių sąrašas>)
- Reikšmė pagal nutylėjimą (<pagal nutylėjimą>), priskiriama atributui, kai vartotojas nepasirenka nei vieno iš išvardintų variantų. Ši reikšmė nėra būtina

Žinias bazėje aprašysime naudojantis Bekaus – Nauro forma (BNF):

```
<klausimu baze>   ::= <klausimas> {, <klausimas>}
<klausimas>       ::= <atributas><lauko tipas><operacija>
                      <klausimo tekstas>
                      <reikšmių sąrašas>
                      [<pagal nutylėjimą>]
<atributas>       ::= ([)<raidė>(]){raidė|skaitmuo}
<reikšmė>         ::= (“)<raidė>(”) {raidė|skaitmuo}
<lauko tipas>     ::= TaipNe | Multi | Multi2 | Pasirinkti | Skaičius|
<klausimo tekstas>::= (“)<raidė>(”){raidė|skaitmuo|skirtukas}
<reikšmių sąrašas>::= <reikšmė> {,<reikšmė>}
```

```
<pagal nutylėjimą> ::= <atributas>=<reikšmė><pasitikėjimas>
<operacija>        ::= CF
<pasitikėjimas>    ::= (@)<skaičius>
<skaičius>         ::= <skaitmuo> {<skaitmuo>}
<raidė>            ::= a | ą | b | c | d | e | ę | ė | f | g | h | i | į | y| j
| k | l | m | n | o | p | q | r | s | š | t | u | ų | ū | v | w | x | z | ž
<skaitmuo>         ::= 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
<skirtukas>        ::= ?
```

2.7.4. Faktų bazė

Faktų bazė, tai sistemoje iš vartotojo gautų atributų ir jų priskirtų reikšmių sąrašas, bei išvadų, kurioms jau yra nustatyti tarpiniai rezultatai. Faktų bazę sudaro:

- Faktai, susidedantys iš atributo ir jo reikšmės
- Identifikuota sritis ir jos išvada
- Svoriniai koeficientai

Žinias bazėje aprašysime naudojantis Bekaus – Nauro forma (BNF):

```
<faktų bazė>       ::= <faktas> {, <faktas>}
                   <išvada> {, <išvada>}
<faktas>           ::= <atributas> <operatorius> <reikšmė> [<pasitikėjimas>]
<atributas>        ::= ([)<raidė>(]){raidė|skaitmuo}
<reikšmė>          ::= (“)<raidė>(”){raidė|skaitmuo}
<pasitikėjimas>    ::= (@)<skaičius>
<išvada>           ::= <sritis>: <rekomendacija> [<pasitikėjimas>]
<skaičius>         ::= <skaitmuo> {<skaitmuo>}
<raidė>            ::= a | ą | b | c | d | e | ę | ė | f | g | h | i | į | y| j
                   | k | l | m | n | o | p | q | r | s | š | t | u | ų | ū | v
                   | w | x | z | ž
<skaitmuo>         ::= 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
<operatorius>      ::= = | < | > | ! | :
```

2.8. Žinių neapibrėžtumų vertinimas sistemoje

Išvadų generatorius sprendimo paieškai turi įvertinti informaciją kuri ne visada yra tiksli. T.y. esant neapibrėžtumui. Projektuojamos sistemos neapibrėžtumo vertinimui naudojamas pasitikėjimo faktorių (*CF*) metodas.

Pasitikėjimo faktoriai skaičiuojami vertinant skirtingus pasitikėjimo faktorius sudurtinei taisyklei, bei dviejų skirtingų taisyklių pasitikėjimo faktorius. Pasitikėjimo faktoriai projektuojamoje sistemoje žymimi skaitine verte.

Galima reikšmių skalė nuo -1 iki +1:

CF=-1 nėra jokio pasitikėjimo;

CF=+1 visiškas pasitikėjimas;

CF=0 nėra nieko žinoma.

Yra visiškas pasitikėjimas kai *CF*=1

Tarkim x_1 ir x_2 yra dvi taisyklės. Naudojami 5 metodai operacijų su taisyklėmis pasitikėjimo faktoriams skaičiuoti:

13 lentelė. Projektuojamos sistemos neapibrėžtumo valdymo metodai

Metodas	Skaičiavimas	Pavyzdys	Aprašymas
Maksimalus	$\min(CF(x_1), CF(x_2))$	$CF(x_1)\ IR\ CF(x_2)$ Kai $CF(x_1)=0,6$ ir $CF(x_2)=0,8$ Rezultatas *CF*=0,6	x_1 ir x_2 turi būti tenkinami, kad taisyklė būtų teisinga. Naudojama, kai taisyklę sudaro du ar daugiau sąlygų, sujungtų IR loginėmis jungtimis, kurių kiekviena turi savo pasitikėjimo faktorių
Minimalus	$\max(CF(x_1), CF(x_2))$	$CF(x_1)\ ARBA\ CF(x_2)$ Kai $CF(x_1)=0,6$ ir $CF(x_2)=0,8$ Rezultatas *CF*=0,8	x_1 arba x_2 turi būti tenkinami, kad taisyklė būtų teisinga. Naudojama, kai taisyklę sudaro du ar daugiau sąlygų, sujungtų ARBA loginėmis jungtimis, kurių kiekviena turi savo pasitikėjimo faktorių
Vidurkis	$(CF(x_1)+CF(x_2))/2$	$CF(x_1)\ IR\ CF(x_2)$ $CF(x_1)\ ARBA\ CF(x_2)$ Kai $CF(x_1)=0,6$ ir $CF(x_2)=0,8$ Rezultatas *CF*=0,7	Maksimumo ir minimumo metodų kompromisas.
Tikimybinė suma	$CF(x_{1_1})+CF(x_{1_2})*(1-CF(x_{1_1}))$	$CF(x_{1_1})=0,7$ iš pirmos taisyklės $CF(x_{1_2})=0,6$ iš antros taisyklės Rezultatas CF=0,88	Naudojama, kai reikia apjungti kelių taisyklių gautos tos pačios išvados pasitikėjimą.
Dauginimas	$CF(x_1)\times CF(x_2)$	*JEI* x_1 *IR* x_2 *TAI* x_3 = 5 su 0,8 pasitikėjimu (prielaida CF=0,9) Rezultatas: x_3 = 5 su CF=0,72	Pasitikėjimas priskirtas taisyklės išvados atributui yra priklausomas nuo prielaidos patikimumo lygio. Naudojama, kai reikia apjungti taisyklei nurodytą $CF(x_2)$ su vartotojo sąlygai nurodytu $CF(x_2)$

CF algoritmai naudojami šiais atvejais:

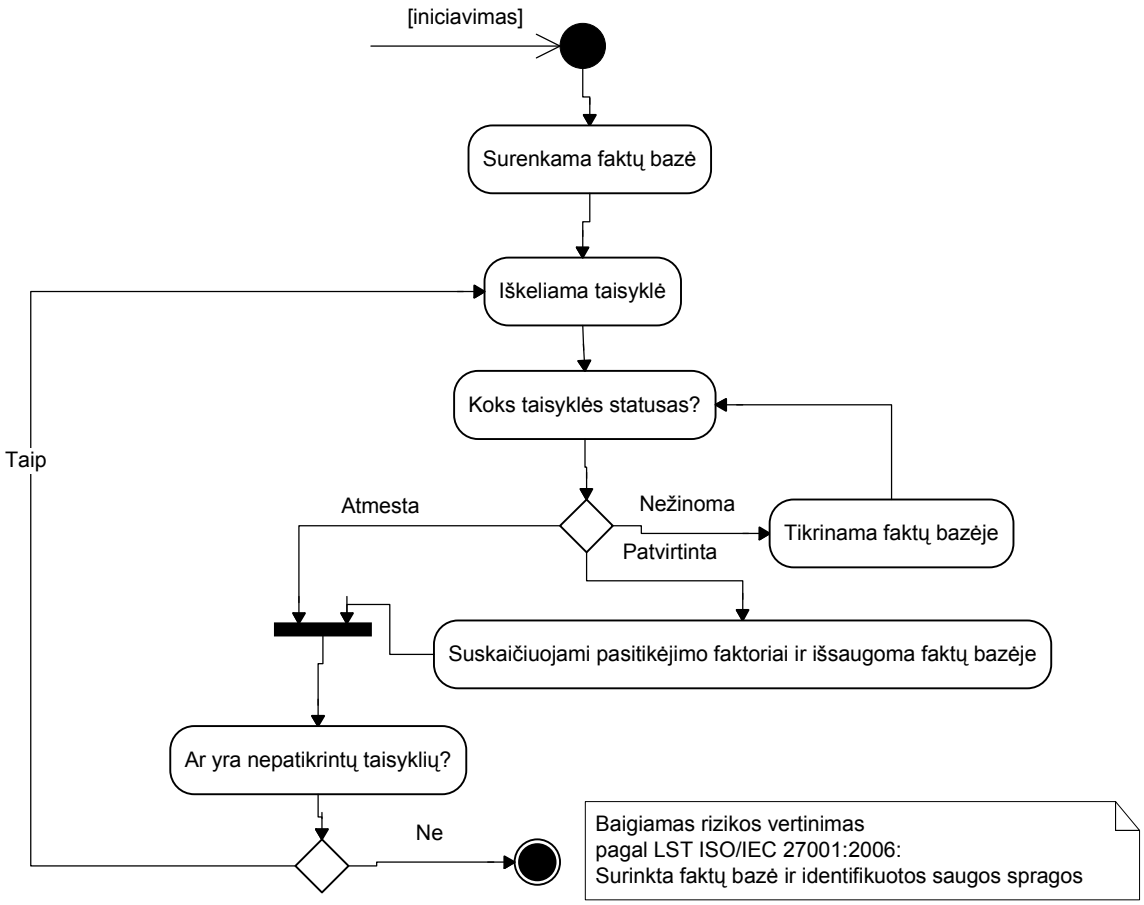
- Pasitikėjimo faktoriai įvedami sistemos vartotojo;
- Pasitikėjimo faktoriai gaunami iš iškeltos taisyklės, susidedantys iš sąlygos pasitikėjimo laipsnio ir taisyklės pasitikėjimo laipsnio;
- Kombinuotas pasitikėjimo faktorius taisyklių, kurias sieja ta pati išvada;
- Bendras pasitikėjimas sprendimo paieškos grandinėje, kuris įtakoja išvadą.

2.9. Sistemos darbo algoritmai

Sprendimų paieškos strategija pasirinkta mišri. Projektuojama sistema naudos:

- tiesioginės grandinės metodą rizikos vertinimui pagal LST ISO/IEC 27001:2006 standarto aprašytas 11 saugos sričių.
- atgalinės grandinės metodą identifikuoti konkrečiai problemai, kad pasiūlytų tinkamą sprendimą.

Išvadų generatoriaus veiksmai su taisyklėmis žinių bazėje ieškant saugumo spragų pavaizduoti darbų sekos diagramoje:

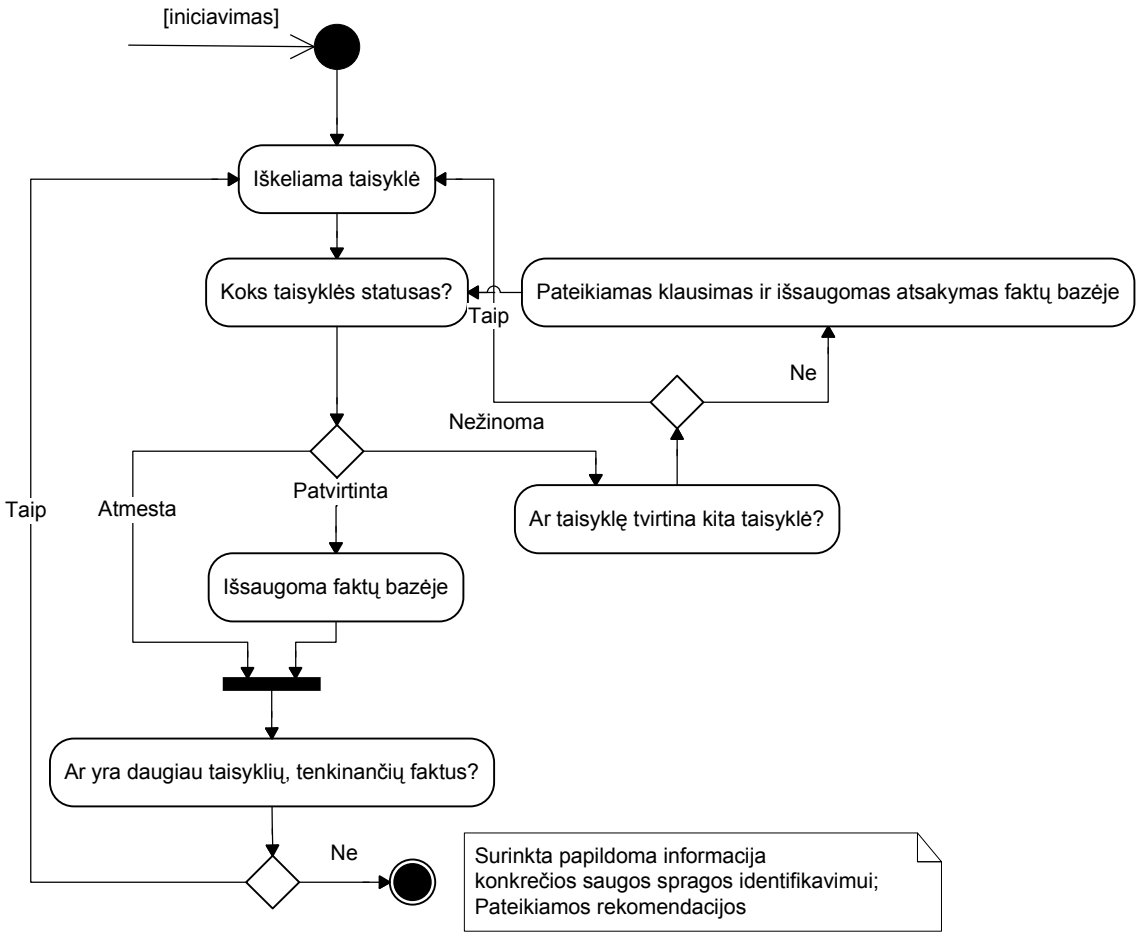


11 pav. UML diagrama: sistemos darbų seka rizikos vertinimui pagal LST ISO/IEC 27001:2006

Pateiktas modelis skirtas vertinti organizacijos saugą pagal LST ISO/IEC 27001:2006 standartą. Čia aptinkamos sritys, kur organizacijos sauga nėra užtikrinta. Naudojama tiesioginės grandinės sprendimų paieškos strategija.

Aptiktoms saugos problemoms spręsti išvadų generatorius pasitelkia kitą mechanizmą sprendimo radimui. Dalis faktų jau gali būti surinkti vykdant saugumo spragų paiešką, kita dalis surenkama klausimų pagalba. Visi duomenys surinkti saugomi faktų bazėje kartu su galimais sprendimais ir jų teisingumas apibrėžiamas procentine išraiška, kurią apskaičiuoja išvadų generatorius. Taisyklių iškėlimo schema pavaizduota pav. 12.

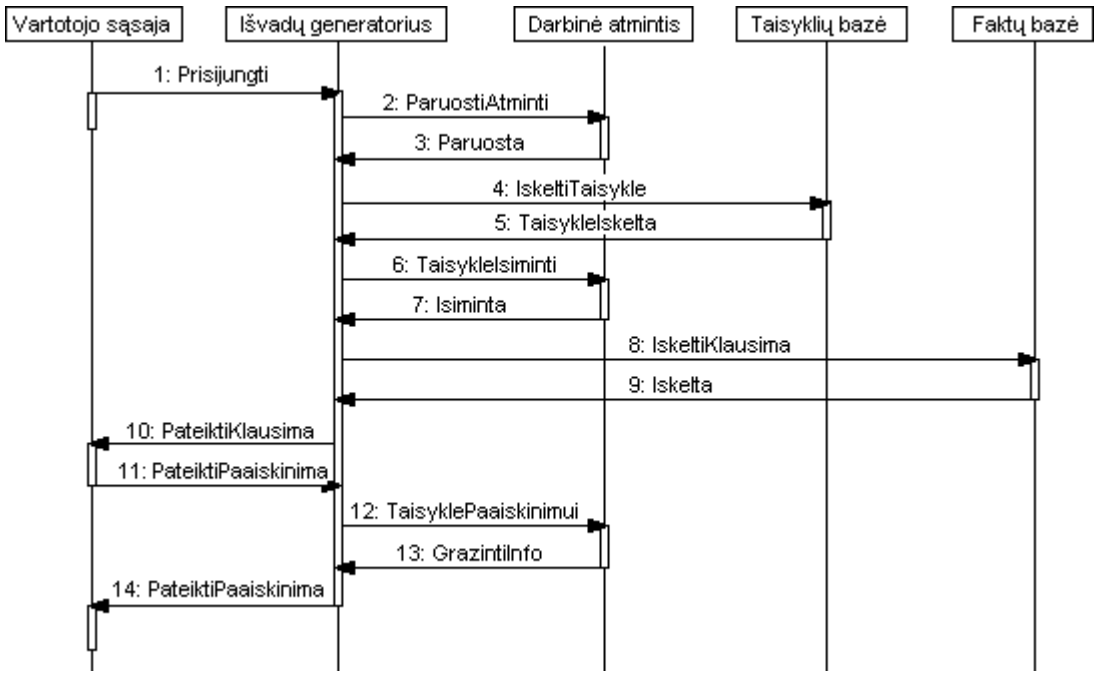
Pavyzdžiui, nėra žinoma, kokio lygio fizinius užraktus turi naudoti organizacija jos maksimaliam saugumui užtikrinti. Tai taisyklių bazė talpina sąrašą galimų fizinių užraktų. O klausimų bazė talpina susijusį klausimyną, kuriame nurodyti fizinių užraktų svoriai esant vienokioms ar kitokioms sąlygoms.



12 pav. UML diagrama: sistemos darbų seka saugumo spragų identifikavimui ir rekomendacijų pateikimui

2.10. Klausimų pateikimas vartotojui – sekų diagrama

Pateiktoje sekų diagramoje atliekama 14 veiksmų, kurie naudojami klausimo pateikimo vartotojui. Visa sesijos su vartotoju informacija saugoma darbinėje atmintyje. Išvadų generatorius kviečia taisykles iš taisyklių bazės pagal savo algoritmus. Vartotojo pateikti duomenys taip pat saugomi darbinėje atmintyje.



13 pav. Klausimų pateikimas vartotojui – sekų diagrama

2.11. Išvados

- Projektavimo etape apibrėžti sistemos tikslai, funkciniai ir nefunkciniai informacijos saugos sprendimų paramos sistemos reikalavimai.
- Sistemoje galimos dvi vartotojo rolės: informacijos saugos auditorius neprofesionalas ir informacijos saugos ekspertas.
- Suprojektuota sistema talpina: žinių bazę ir faktų bazę. Žinių bazę sudaro: taisyklių, klausimų ir išvadų bazės. Faktų bazė yra skirta talpinti audito duomenims audito metu, bei ankstesnių auditų išvadų saugojimui.
- Žinių atvaizdavimui žinių bazėje pasirinktas taisyklių formavimo metodas. Žinios bazėje aprašytos Backus-Nauru (BNF) forma.
- Neapibrėžtumų valdymui sistemoje pasirinktas pasitikėjimo faktorių metodas, kuris leidžia nurodyti atributams, taisyklėms, atsakymams ir bendram sistemos pasitikėjimo laipsniui vertes reikšmių skalėje nuo -1 iki +1.
- Sprendimų paieškos strategija pasirinkta mišri. Suprojektuota sistema naudos tiesioginės grandinės metodą rizikos vertinimui pagal LST ISO/IEC 27001:2006 standarto aprašytas 11 saugos sričių. Sistema naudos atgalinės grandinės metodą identifikuoti konkrečiai problemai, kad pasiūlytų tinkamą sprendimą.

3. INFORMACIJOS SAUGOS AUDITO SPRENDIMŲ PARAMOS SISTEMOS PROTOTIPO REALIZAVIMAS

3.1. Sistemos prototipo realizavimo įrankio pasirinkimas

Informacijos saugos audito sprendimų paramos sistemos prototipui realizuoti naudosime ekspertinių sistemų kūrimo priemones. Ekspertinių sistemų apvalkalai – tai tuščios ekspertinės sistemos, kurias duomenimis užpildo pats vartotojas.

FuzzyCLIPS [13]

- FuzzyCLIPS yra taisyklėmis paremtas apvalkalas skirtas pristatyti ir manipuliuoti neraiškiais (fuzzy) faktais ir taisyklėmis. FuzzyCLIPS funkcionalumas leidžia operuoti tiksliai ir netiksliais faktais, taip pat vienu metu naudoti kombinuotą sprendimų priėmimo būdą, leidžianti ekspertinei sistemai naudoti maišytas taisykles ir faktus.
- Galima naudoti moksliniais ir tyrimų tikslais.
- FuzzyCLIPS kuriamas su Microsoft VC++ 6.0 arba Borland C++ 4.51.
- Sukurta ekspertinė sistema diegiama į vartotojo kompiuterį ir vartotojas naudotis ja kaip Web aplikacija neturi galimybės.

CLIPS [6]

- Ekspertinių sistemų kūrimo įrankis, kuris suteikia išbaigtą aplinką kuriant taisyklėmis ir/arba paremtas ekspertines sistemas.
- Sukurta dar 1985 metais ir iki šiol plačiai naudojama vyriausybėje, pramonėje ir akademinėje veikloje.
- CLIPS įrankis palaiko tris skirtingas programavimo paradigmas: taisyklėmis paremtas, į objektą orientuotos ir procedūrinės. Taisyklėmis paremtas programavimas leidžia operuoti veiksmų seka pagal pateiktą situaciją. Į objektus orientuotas programavimas leidžia kompleksinę sistemą būti sumodeliuotą iš skirtingų modulinių komponentų (kurie gali būti lengvai naudojami modeliuojant kitas sistemas ar kuriant naujus komponentus). Procedūrinio programavimo galimybės yra panašios kaip ir C, Java kalbose.
- Kita savybė – portatyvumas: CLIPS parašyta C kalba ir gali būti diegiama skirtingose operacinėse sistemose, įskaitant Windows XP, MacOS X ir Unix. CLIPS gali būti perkelta į bet kokią sistemą, naudojančią C arba C++ kompiliatorių.
- Integracija ir plėtimas: CLIPS gali būti integruota su kalbomis, tokiomis kaip Java.

- CLIPS yra skirta viešam naudojimui programinė įranga, nereikalaujanti licenzijos ir paskutinį kartą atnaujinta 2008 metais.

e2gLite [4]

- e2gLite ekspertinių sistemų apvalkalas yra Java applet‘as, kuri integruojama į internetinį puslapį ir parsiunčiama iš interneto serverio per vartotojo naršyklę. Applet‘as pakrauna žinių bazę iš serverio ir vaizduojamas naršyklėje.
- Svarbi e2gLite savybė yra prieinamumas. Kadangi žinių bazės failai įkeliami į vartotojo naršyklę, tai 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).
- e2gLite pasižymi savo paprastumu ir lankstumu. Java applet‘ą yra taip pat lengva įterpti į interneto puslapį kaip grafinį vaizdą arba įtraukti į HTML lentelės langelį, sutiekiant galimybę lanksčiam puslapio formatavimui ir ekspertinės sistemos integravimu į kitą turinį.
- Trūkumas: kol java applet‘as keliamas į naršyklę pirmą kartą vartotojui reikia palaukti vidutiniškai 10 sekundžių (priklausomai nuo interneto greičio). Pakrovimo laikas tiesiogiai priklauso nuo failo dydžio. Vieną kartą pakrautas applet‘as gali būti naudojamas su skirtingomis duomenų bazėmis keliuose languose arba daug kartų tame pačiam lange nereikalaujant perkrovimo. Dėl startavimo laiko e2gLite dažniausiai naudojama mažas duomenų bazes turinčioms ekspertinėms sistemoms.
- Žinių bazė yra tekstinis failas, skaitomas iš internetinio serverio su Java applet‘u. Ji yra viešo pobūdžio, todėl negali būti laikoma konfidencialia.
- e2gLite ekspertinių sistemų apvalkalas yra visiškai nemokamas ir gali būti naudojamas komercinei veiklai.

Jess [23]

- Java kalba parašytas ekspertinių sistemų apvalkalas.
- Žinių bazėje žinios atvaizduojamos taisyklių forma. Galimi du variantai atvaizdavimui: naudojantis specialia JESS taisyklių kalba arba XML forma.
- Žinios aprašomos gali būti dviem būdais: taisyklėmis, arba naudojant predikatų logiką.
- Išvadų generatorius sprendimų paieškau naudoja tiesioginės grandinės metodą.

- JES apvalkalas neturi neapibrėžtumų vertinimo mechanizmo. UncertaintyJess išplėtimas neapibrėžtumams vertinti naudoja pasitikėjimo faktorius pagal MYCIN.
- Teigiama, kad akademiniam naudojimui galima nemokama versija, bet jos nepavyko gauti. Galima laisvai prieinama bandomoji versija 30 dienų naudojimui.

14 lentelė. Ekspertinių sistemų apvalkalų palyginimas

Ekspertinių sistemų apvalkalas	Žinių atvaizdavimas žinių bazėje	Neapibrėžtumų vertinimas	Sprendimų paieškos strategija	Programavimo kalba	Prieinamumas
FuzzyCLIPS	• neraiški logika, • taisyklių formavimas	• neapibrėžtų aibių teorija • pasitikėjimo faktoriai	• tiesioginės grandinės metodas, • atgalinės grandinės metodas	C kalba	Nemokama nekomerciniams tikslams
CLIPS	• taisyklių formavimas	Nepalaiko	• Tiesioginės grandinės metodas	C kalba, galima integracija su Java	Nemokama nekomerciniams tikslams
e2gLite	• taisyklių formavimas	• pasitikėjimo faktoriai	• tiesioginės grandinės metodas, • atgalinės grandinės metodas	Java	Nemokama nekomerciniams tikslams
Jess	• taisyklių formavimas • predikatų logika	• UncertaintyJess išplėtimas naudoja pasitikėjimo faktorius	• Tiesioginės grandinės metodas	Java	Nemokama nekomerciniams tikslams. Nepavyko gauti nemokamos versijos

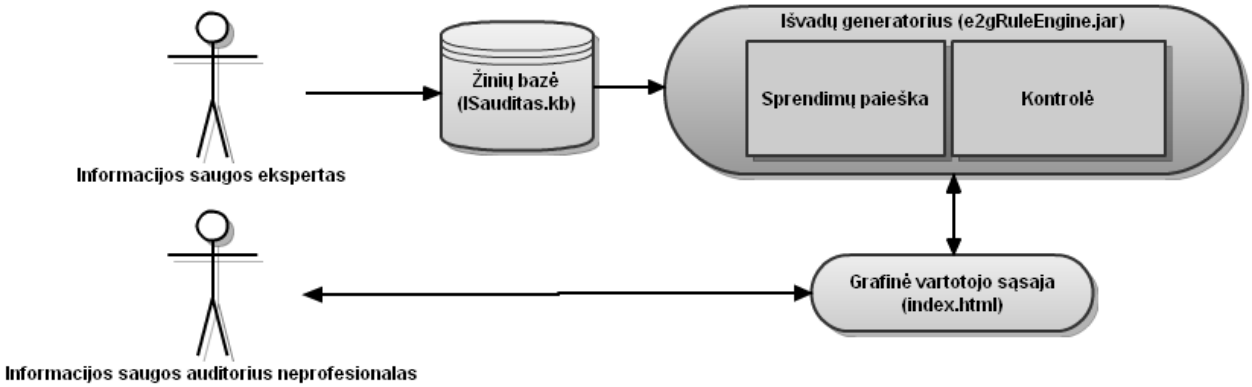
Pasirinkau e2gLite ekspertinės sistemos apvalkalą ekspertinės sistemos kūrimui ir pritaikymui informacijos saugos auditui atlikti, nes jis tenkina visus iškeltus reikalavimus sistemai: jį lengva vystyti, naudoja du sprendimų priėmimo algoritmus, be to veikia web aplinkoje, kas leidžia vartotojui bet kada prieiti prie sistemos ir atlikti testus jo kompiuterio saugumui patikrinti bei gauti rekomendacijas. Pagrindinis sistemos pliusas yra tas, kad nereikalauja diegti programinės įrangos į vartotojo kompiuterį.

3.2. Sistemos prototipo architektūra

Informacijos saugos sprendimų paramos sistemą sudaro:

- išvadų aparatas (e2gRuleEngine.jar);
- žinių bazė (ISauditas.kb);
- grafinė vartotojo sąsaja (index.html);

Jos architektūra pateikta 14 paveiksle [4].



14 pav. Sistemos prototipo architektūra

Grafinę vartotojo sąsają turi tik informacijos saugos auditorius, informacijos saugos ekspertas žinių pildymą atlieka tiesiogiai žinių bazėje. Be to, žinių bazės klausimai, taisyklės ir rekomendacijos nėra išskirtos, ir saugomos vienoje vietoje.

3.3. Žinių bazės taisyklių struktūra

Žinių bazės taisyklės e2glite ekspertinių sistemų apvalkale formuojamos specialia e2glite kalba. Kur viename .kb tipo faile yra saugoma: taisyklės, išvados ir klausimynas.

Taisyklės. Taisyklę identifikuoja operatorius RULE. Pasitikėjimas yra priskiriamas pačiai taisyklei. Sąlygai suteikiamas pasitikėjimas tuo atveju, kai sąlyga yra kitos, prieš tai iškeltos taisyklės išvada. Taisyklių aprašymo pavyzdys:

```
RULE [9.1.4]
If [Saugos politikos dokumentas]="yra" and
[9-1]!"Prieigos saugos reikalavimai" and
[9-1]!"Nėra aprašyta"
Then   [Netinkama saugos politika] = "Reikia peržiūrėti kompiuterinės įrangos išdėstymo
ir montavimo politiką" @10 and
```

```
      [Netinkama saugos politika] = "Fizinės prieigos prie įrangos valdymas turi būti peržiūrėtas iš naujo" @10 and
      [Netinkama saugos politika] = "Reikia peržiūrėti bendrą kompiuterinių sistemų saugumo politiką" @60 and
      [Netinkama saugos politika] = "Slaptažodžių politika turi būti peržiūrėta" @60
```

Taisyklės formuojamos artima žmonių kalbai forma, t.y. sudaryta iš sąlygos sakinio Jei-Tai (If-Then). Taip pat galimi naudoti operatoriai and (ir), or (arba), ! (neigimas), : (bet kuris iš išvardytų). Taisyklės Then dalyje yra galima nurodyti išvados pasitikėjimą esamomis aplinkybėmis.

Klausimynas. Klausimynas yra formuojamas tame pačiame faile. Klausimas identifikuojamas naudojant operatorių PROMT. Čia galima nurodyti pateikiamo vartotojui lauko atsakymui pažymėti tipo (MultiChoice nurodo lauką, kuriame leidžiama pasirinkti vieną iš daugelio), bei galimybę vartotojui nurodyti savo pasitikėjimą atsakymu (CF). Tada pateikiamas klausimo tekstas kabutėse, bei galimi atsakymo variantai. Galima nurodyti atsakymą pagal nutylėjimą, jei vartotojas nežino atsakymo, bei tam atsakymui nurodyti pasitikėjimo faktorių. Klausimo aprašymo pavyzdys pateiktas:

```
PROMPT [8-1] MultChoice CF
"Ar yra laikomasi saugos politikos dokumente nurodytų fizinės ir aplinkos saugos reikalavimų?"
"Taip"
"Ne"
"Ne visų"
DEFAULT [8-1] = "Ne visų"
```

Išvados. Identifikatorius GOAL žymi išvadą, kuri bus teikiama vartotojui. T.y. išvados sritis, o pats tekstas yra imamas iš taisyklės, kuri turi nurodytą išvados sritį. Vienos išvados skirtos identifikuoti saugos spragai, o kitos skirtos pateikti su ta spraga susijusios išvados rekomendacijai.

```
GOAL [Netinkama saugos politika]
GOAL [Netinkama saugos politika: rekomendacija]
GOAL [Netinkama fizinė ir aplinkos sauga]
GOAL [Netinkama fizinė ir aplinkos sauga: rekomendacija]
GOAL [Netinkamas komunikacinių kanalų ir procesų valdymas]
GOAL [Netinkamas komunikacinių kanalų ir procesų valdymas: rekomendacija]
GOAL [Netinkama prieigos kontrolė]
GOAL [Netinkama prieigos kontrolė: rekomendacija]
```

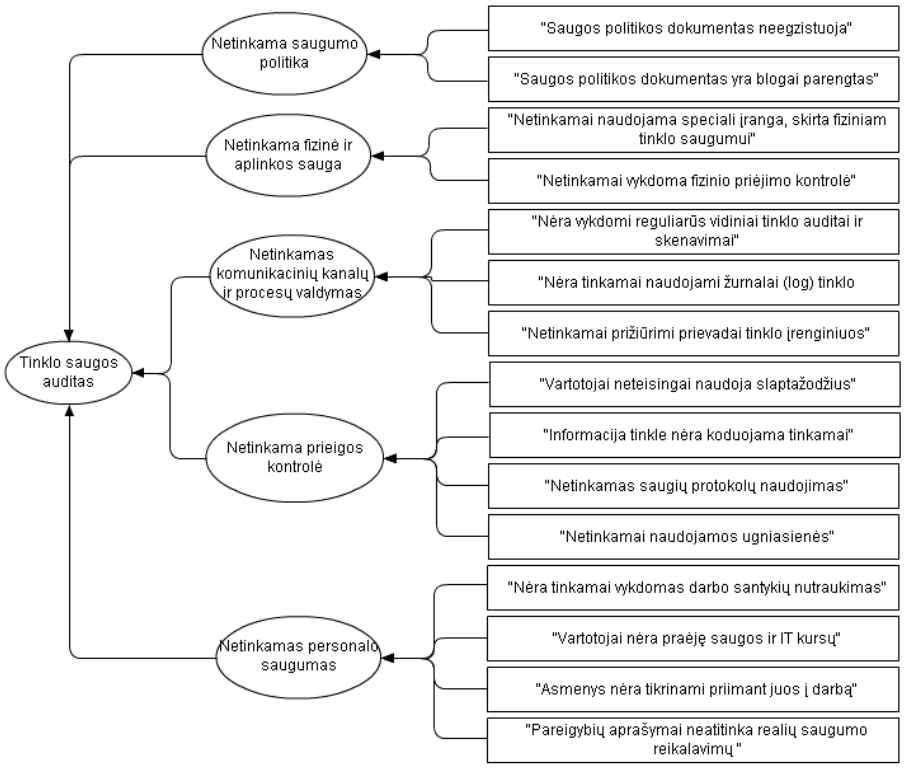
```
GOAL [Netinkamas personalo saugumas]
```

3.4. Realizuotos žinių bazės priklausomybių diagramos

Realizuojant tinklo saugos įvertinimo žinių bazę pirmiausia buvo apsibrėžtos galimos tinklo saugos spragos ir galimos rekomendacijos, grėsmėms sumažinti. Informacijos saugos audito sprendimų paramos sistema, ieškodama rekomendacijų turi praeiti kelis tikrinimo žingsnius:

1. Identifikuoti grėsmę tinklo saugai keliančias informacijos saugos sritis pagal LST ISO/IEC 27001:2006 standartą bei tos srities priežastį
2. Rasti atitinkamos srities konkrečias saugos spragas ir pateikti tinkamą rastos priežasties sprendimo rekomendaciją

Žemiau yra pateikta realizuotos žinių bazės priklausomybių diagrama, vaizduojanti informacijos saugos auditui išskirtas rizikos sritis. Rekomenduojamas veiksmas bus tuo tikslesnis, kuo didesnis bus faktų bagažas, žinoma, priklausomai nuo problemos sudėtingumo.



15 pav. Sistemoje išskirtų informacijos saugos rizikos sričių priklausomybių diagrama

Pirma automatizuotos informacijos saugos sprendimų paieškos sistemos užduotis yra identifikuoti grėsme keliančias sritis. Tam, kad informacijos saugos auditas atitiktu LST ISO/IEC

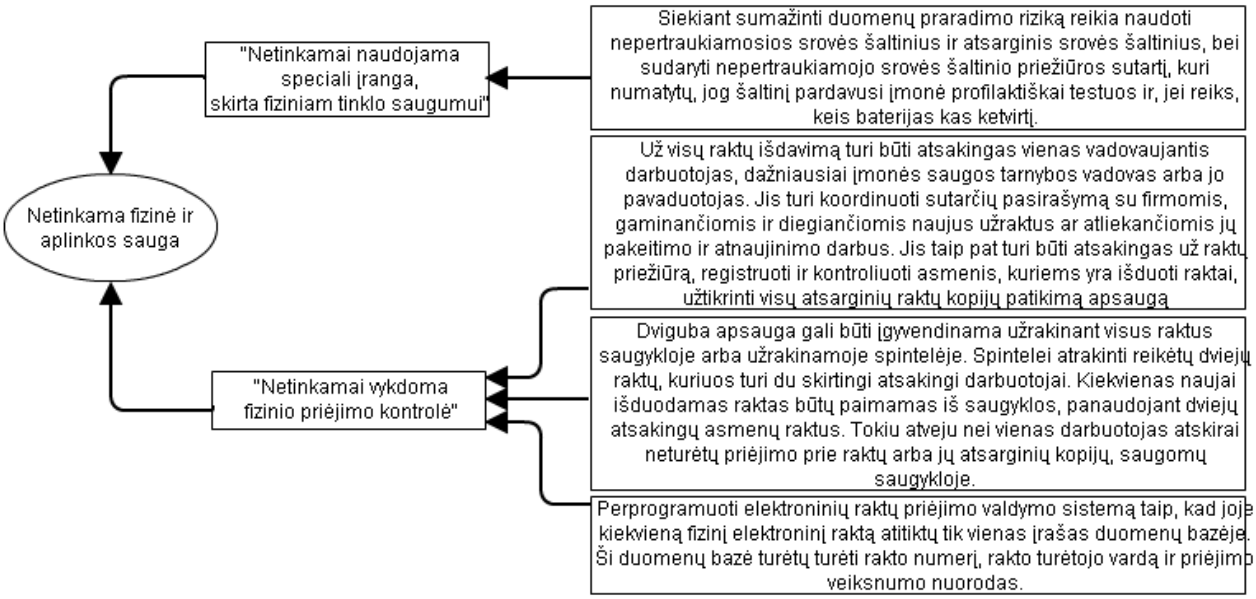
27001:2006 standartą, buvo pasinaudota standarte analizuojamomis saugos sritimis. Iš 11 standarte analizuojamų sričių buvo pasirinktos 5:

- Saugumo politika
- Fizinė ir aplinkos sauga
- Komunikacinių kanalų ir procesų valdymas
- Prieigos kontrolė
- Personalo sauga

Šios rizikos sritys dar išskirstytos į 15 galimų saugumo spragų. Atliekant auditą sistemos pirmas žingsnis ir yra apklausos metu surinkti faktus ir nustatyti organizacijos tinkle egzistuojančias saugos spragas.

Šitas sritis ir jų galimas priežastis sistema identifikuoja pasinaudodama neraiškios logikos metodais. Faktų bazė renkama tam, kad remiantis jais būtų galima identifikuoti vieną iš sričių ir jo priežasčių. Atlikus tokią analizę kiekvienos srities priežasčiai yra apskaičiuojamas tikėtinumo faktorius. Jei tas faktorius yra mažesnis nei minimalus nurodytas sistemos pasitikėjimo faktorius, tuomet laikoma, kad sritis yra saugi ir toliau nagrinėti nereikia. Priešingu atveju yra vykdomas antras žingsnis.

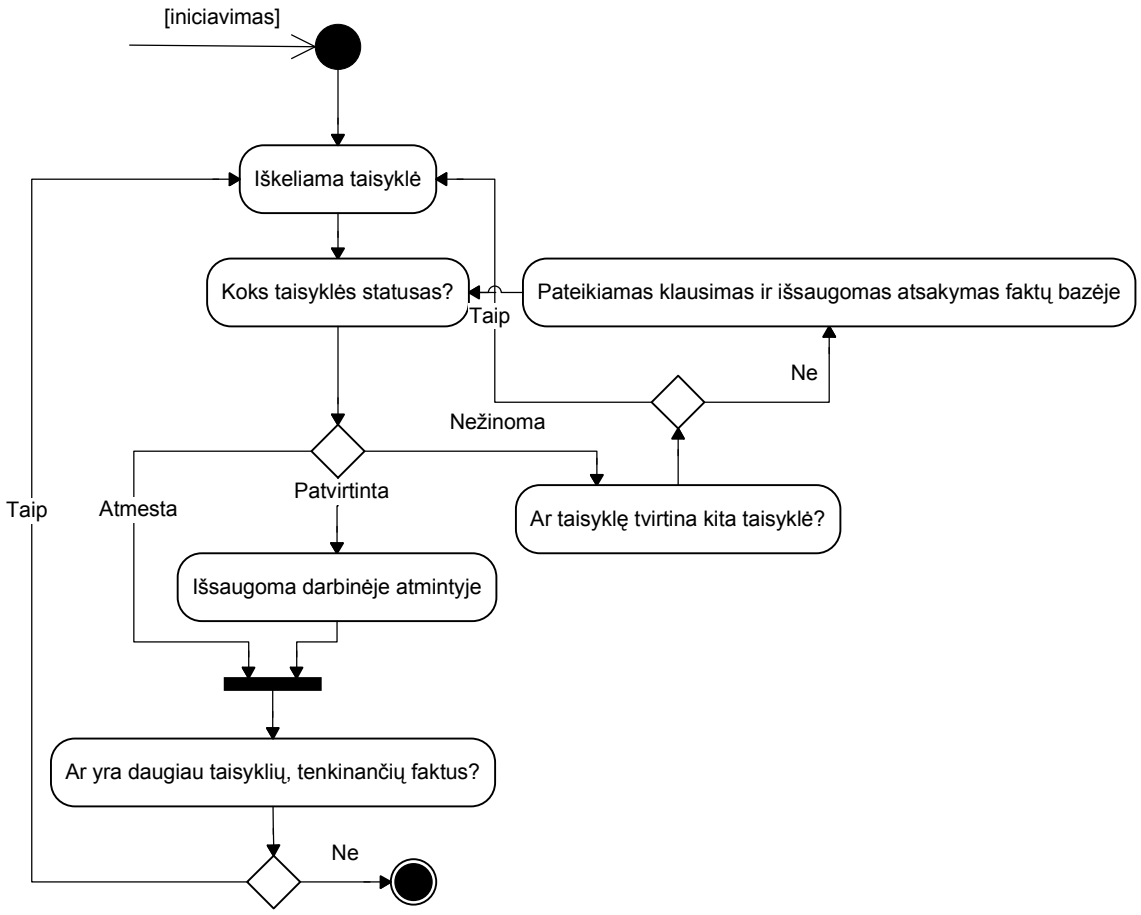
Antrame žingsnyje yra bandoma surinkti daugiau informacijos apie galimą nagrinėjamą sritį, kad galima būtų pateikti rekomendacijas iš galimų rekomendacijų sąrašo. Kiekviena pirmame žingsnyje identifikuota saugos srities spraga turi galimą bazę rekomendacijų. Tam pirma reikia ištirti tikslią saugos spragą ir pateikti atitinkamą rekomendaciją. Pateiktoje priklausomybių diagramoje yra pavaizduotos realizuotos fizines ir aplinkos saugos srities rekomendacijos.



16 pav. Sistemoje realizuotų rekomendacijų atitinkamoms saugos spragoms mažinti priklausomybių diagrama

3.5. Sprendimų paieška žinių bazėje

Sukurtos žinių bazės sprendimų paieškos strategijos loginė schema pateikta paveiksle 17. Sistema sprendimo suradimui iškelia rezultatą kurį reikia patvirtinti ir ieško susijusių taisyklių. Jei klausimas atitinka iškeltą taisyklę ir pripažįstamas kaip teisingu, yra tikrinamos kitos taisyklės tam rezultatui užtikrinti ir jis keliauja tolesne klausimų grandine tolyn, kol nebelieka klausimų, virtinančių rezultatą. Jei klausimas atitinka iškeltą taisyklę ir pripažįstamas kaip neteisingu, tuomet iš karto galime apspręsti rezultatą, bet tai nereiškia, kad bus baigiamas testas. Testas vykdomas tol, kol patikrinami visi galimi rezultatai. Kiekvieną kartą iškeliant taisyklę yra tikrinamas jos statusas: „nežinoma“, „patvirtina“ ar „atmesta“. Jei statusas yra „nežinoma“, tuomet yra tikrinamos kitos susijusios taisyklės ar renkami faktai klausimų pagalba iš vartotojo, kol statusas tampa „patvirtinta“ arba „atmesta“.



17 pav. UML diagrama: sistemos darbo algoritmas

Sistema naudoja kombinuotą sprendimų paieškos metodą, t.y. apjungti tiesioginės ir atgalinės grandinės metodai. Inicijuojant žinių bazę yra iškeliama pirma taisyklė, kaip rezultatas paimama jos „Then“ dalis ir bandoma įrodyti kitų taisyklių pagalba. Taisyklėms, kurios yra lygiavertės rezultato atžvilgiu, iškelti yra naudojamas tiesioginės grandinės metodas.

Taip pat sistemoje yra galimybė parinkti sprendimų paieškos būdą, kai pirmiausia yra paimamas rezultatas ne iš taisyklės „Then“ dalies, o pirma išvada iš išvadų sąrašo, ir bandoma ją įrodyti.

3.6. Sistemos prototipo tyrimas

Informacijos saugos audito sprendimų paramos sistemoje galimos dvi vartotojų rolės: informacijos saugos auditorius neprofesionalas (atliekantis auditą) ir informacijos saugos ekspertas (kuriantis žinių bazę). Sistemos prototipas neturi vartotojo sąsajos, skirtos ekspertui,

žinių bazės pildymui, todėl jam reikia išmanyti žinių aprašymo kalbą. Ji nėra sudėtinga, bet reikalauja minimalių apmokymų.

3.6.1. Sistemos vartotojo sąsaja

Realizuota sistema yra žiniatinklio programa, taigi vartotojams pasiekiama per interneto naršyklę. Vartotojams prireikus pasinaudoti sistema, nereikia diegti jokių papildomų įrankių į kompiuterį, reikalinga tik prieiga prie interneto bei kompiuteryje turi būti leidžiama naudoti Java Server Pages (CGI), Active Server Pages (ASP), Common Gateway Interface (SGI). 18 paveiksle pavaizduota sistemos vartotojo sąsaja.

18 pav. Sistemos vartotojo sąsaja: klausimo pateikimas

Meniu punktai:

- Pradėti testavimą – audito sistemos inicijavimas
- Apie sistemą – pateikiama bendra informacija apie sistemą

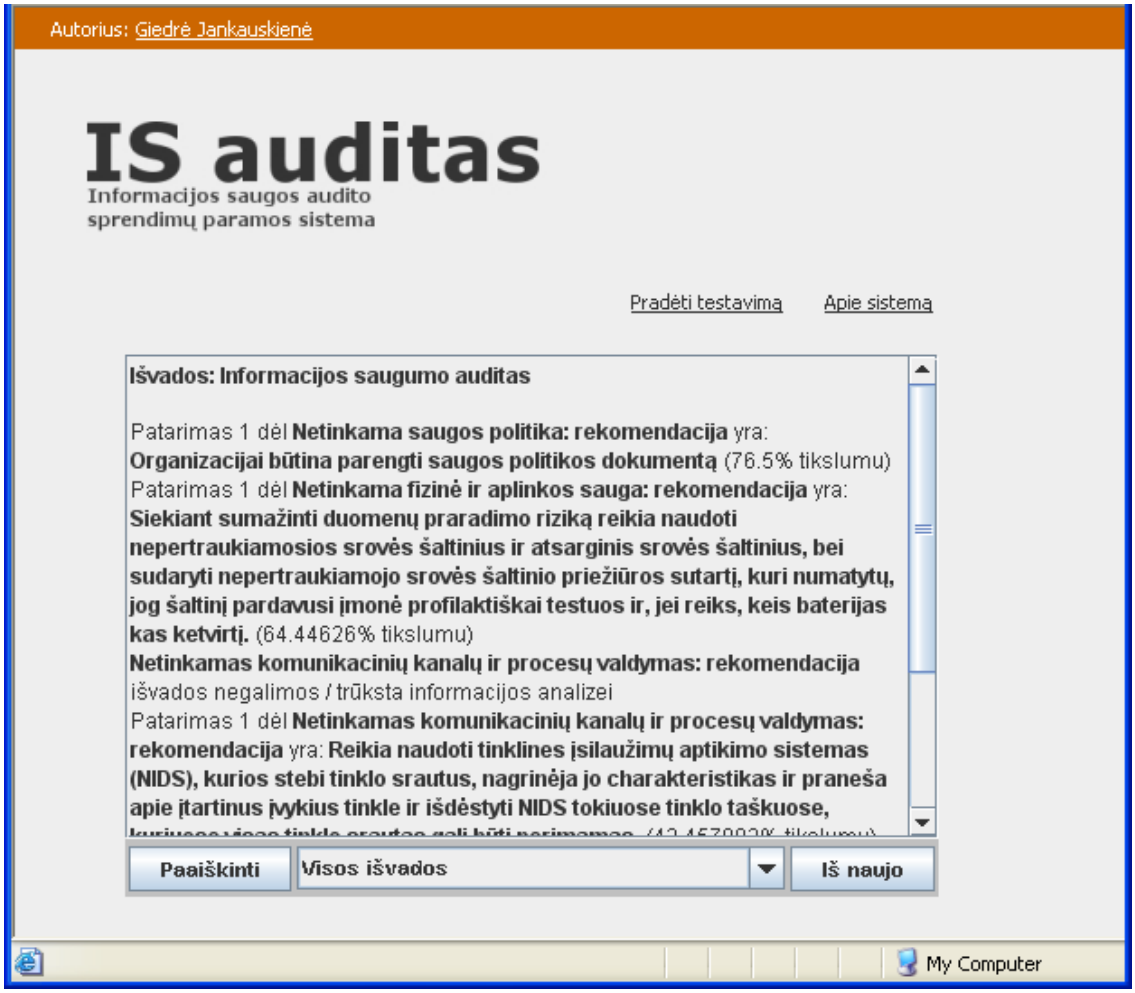
Paveiksle pavaizduotas sistemos vartotojui pateikiamo klausimo pavyzdys. Čia vartotojas gali:

- parinki atsakymo variantą (-us);
- nurodyti savo parinkto varianto tikslumą nuo 50% iki 100%;
- patvirtinti atsakymą mygtuku „Gerai“;
- patikrinti, kodėl yra užduotas toks klausimas mygtuku „Kodėl?“. Jis pateikia vartotojui taisyklę, kurią sistema nori patikrinti užduodama klausimą. žr. Pav. 19;
- pradėti testą nuo pradžių mygtuku „Iš naujo“.

19 pav. Sistemos vartotojo sąsaja: klausimo paaiškinimo pateikimas

3.6.2. Sistemos rekomendacijų pateikimas vartotojui

Informacijos saugos auditorius neprofesionalui atliktus auditą sistema pateikia rekomendacijas. Rekomendacijos pateikiamos kaip pavaizduota 20 paveiksle.



20 pav. Sistemos vartotojo sąsaja: rekomendacijų pateikimas vartotojui

Rekomendacijos yra pateikiamos kartu su identifikuota spraga. Pvz.: sistema identifikavo, kad organizacijoje netinkama fizinė ir aplinko sauga. Ir tiksliau išsiaiškinus problemą siūlo: „Siekiant sumažinti duomenų praradimo riziką reikia naudoti nepertraukiamos srovės šaltinius ir atsarginės srovės šaltinius, bei sudaryti nepertraukiamos srovės šaltinio priežiūros sutartį, kuri numatytų, jog šaltinį pardavusi įmonė profilaktiškai testuos ir, jei reiks, keis baterijas kas ketvirtį.“ Taip pat pateikiamas rekomendacijos tikslumas, šiuo atveju tai 64%.

Sistema pateikia rekomendacijas tekstine forma.

Žemiau pateiktame paveiksle pavaizduotas atvejis, kai informacijos sauga tenkina visus saugos reikalavimus pagal surinktus faktus ir taisykles žinių bazėje. Tuomet sistema rekomendacijų jokių pateikti negali.

21 pav. Sistemos vartotojo sąsaja: rekomendacijų pateikimas vartotojui esant maksimaliam saugumui

3.6.3. Sistemos rekomendacijų paaiškinimo pateikimas vartotojui

Atlikus testą vartotojas gali peržiūrėti sistemos ir vartotojo veiksmus, atliktus sprendimo paieškos metu. Kartu su nagrinėjamais iškeltais klausimai pateikiami ir skaičiavimai, kurie buvo naudojami išvados tikslumui apskaičiuoti.

22 pav. Sistemos vartotojo sąsaja: rekomendacijų paaiškinimo pateikimas

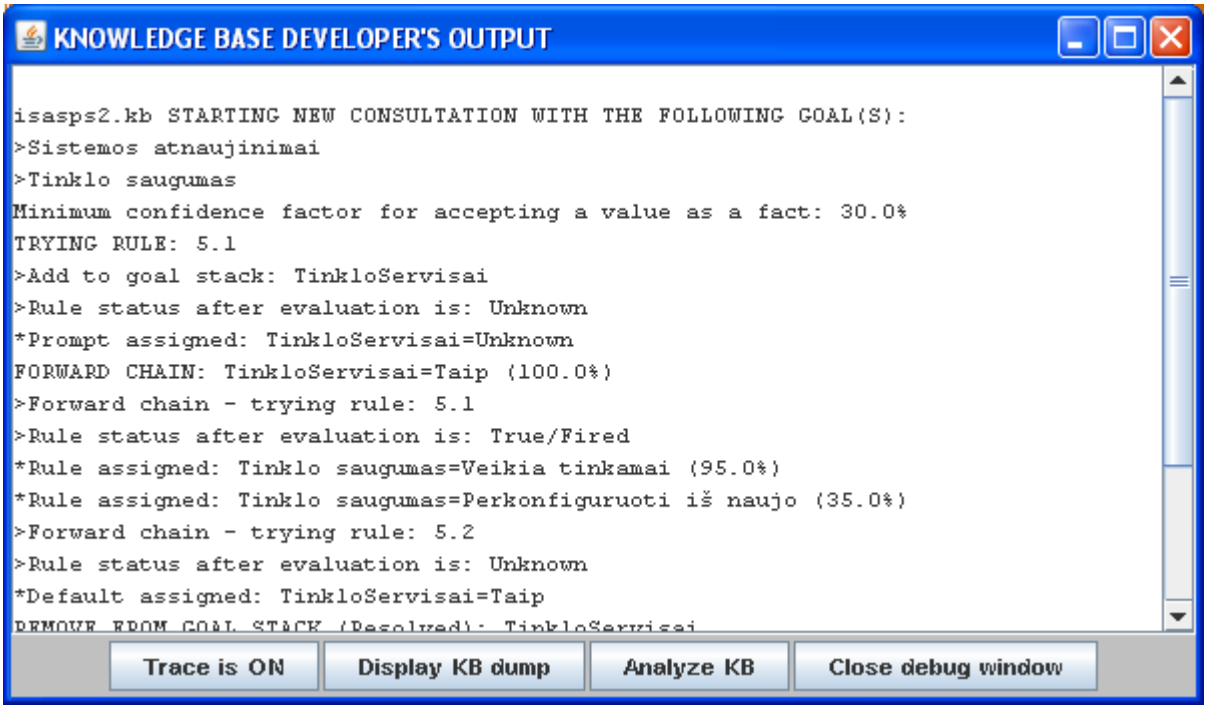
3.6.4. Žinių bazės išvesties funkcijos

Sistemoje atliktus papildomus nustatymus, t.y. yra galimybė HTML faile nurodyti žinių bazės išvesties lango įjungimą. Jis suteikia papildomas funkcijas sistemos analizei:

1. Vykdomo testo išvadų generatoriaus atliekamų veiksmų einamuoju metu pateikimas
2. Pateikiama žinių bazės kopija
3. Žinių bazės analizės langas

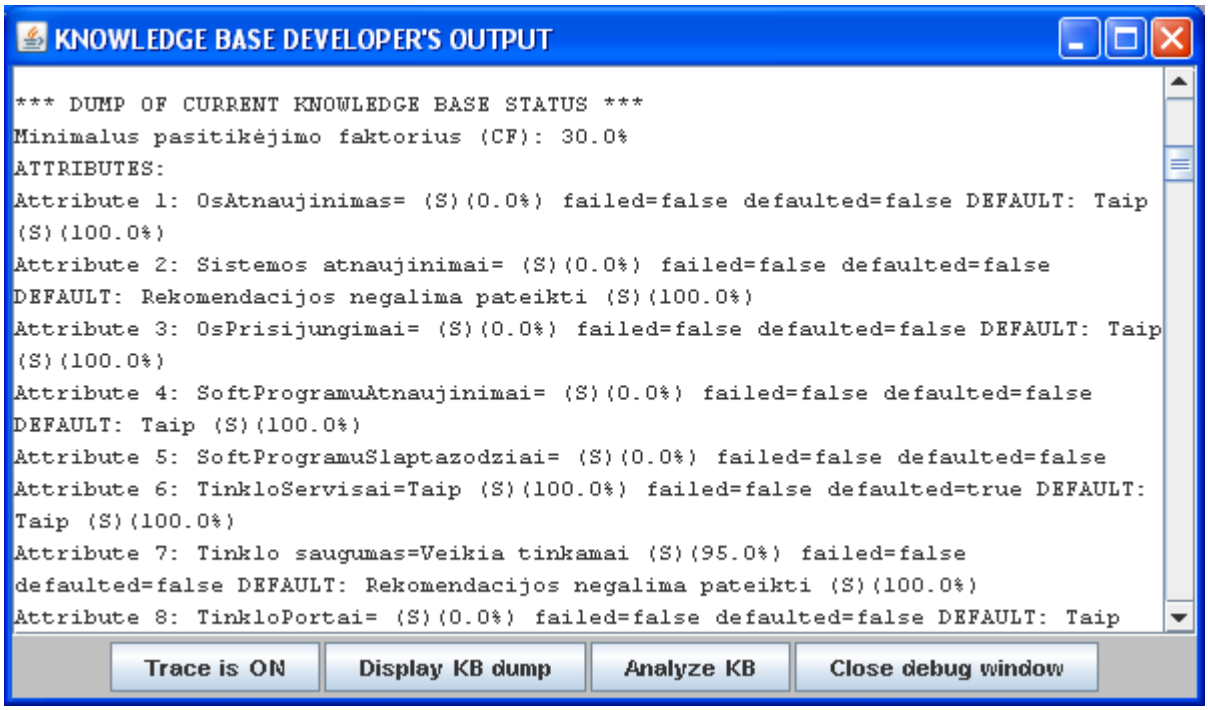
1. Vykdomo testo išvadų generatoriaus atliekami veiksmai pateikimo pavyzdys pateiktas pav. 23. Sistema pirmiausia nustato, kokios išvados yra galimos, koks minimalus pasitikėjimas bus užskaitomas kaip teisingus ir pateikiamas vartotojo rezultatuose. Jei pasitikėjimas bus mažesnis nei nustatytas minimalus pasitikėjimas, tuomet tokia išvada bus nepateikiama vartotojui kaip išvada.

Tuomet surandama taisyklė, kuria bandoma patvirtinti. Po atsakymo išvadų generatorius tikrina, ar taisyklė patvirtinta ar paneigta, jei jos statusas nėra žinomas, tikrinami kitos sąlygos.



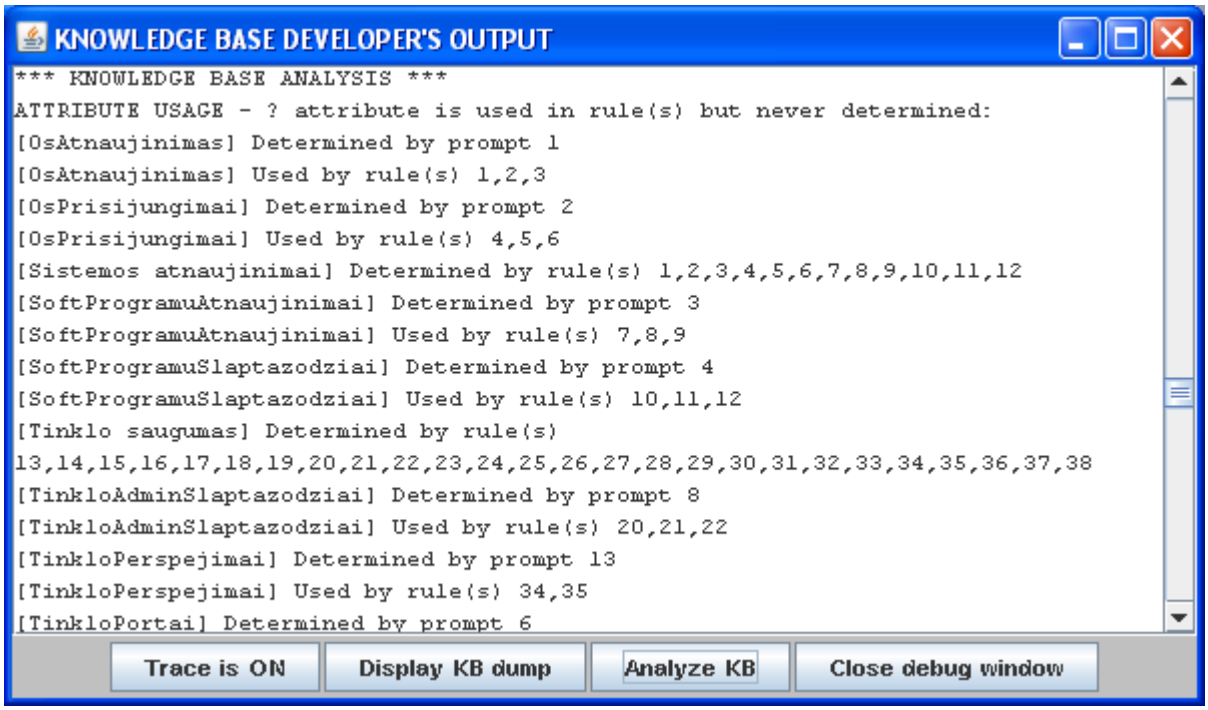
23 pav. Išvadų generatoriaus atliekami veiksmai audito metu

2. Pateikiama žinių bazės kopija. Čia sistema iš žinių bazės pateikia išgrynintą informaciją: Atributus, jų galimas reikšmes, taisykles ir išvadas



24 pav. Žinių bazės kopijos pateikimas

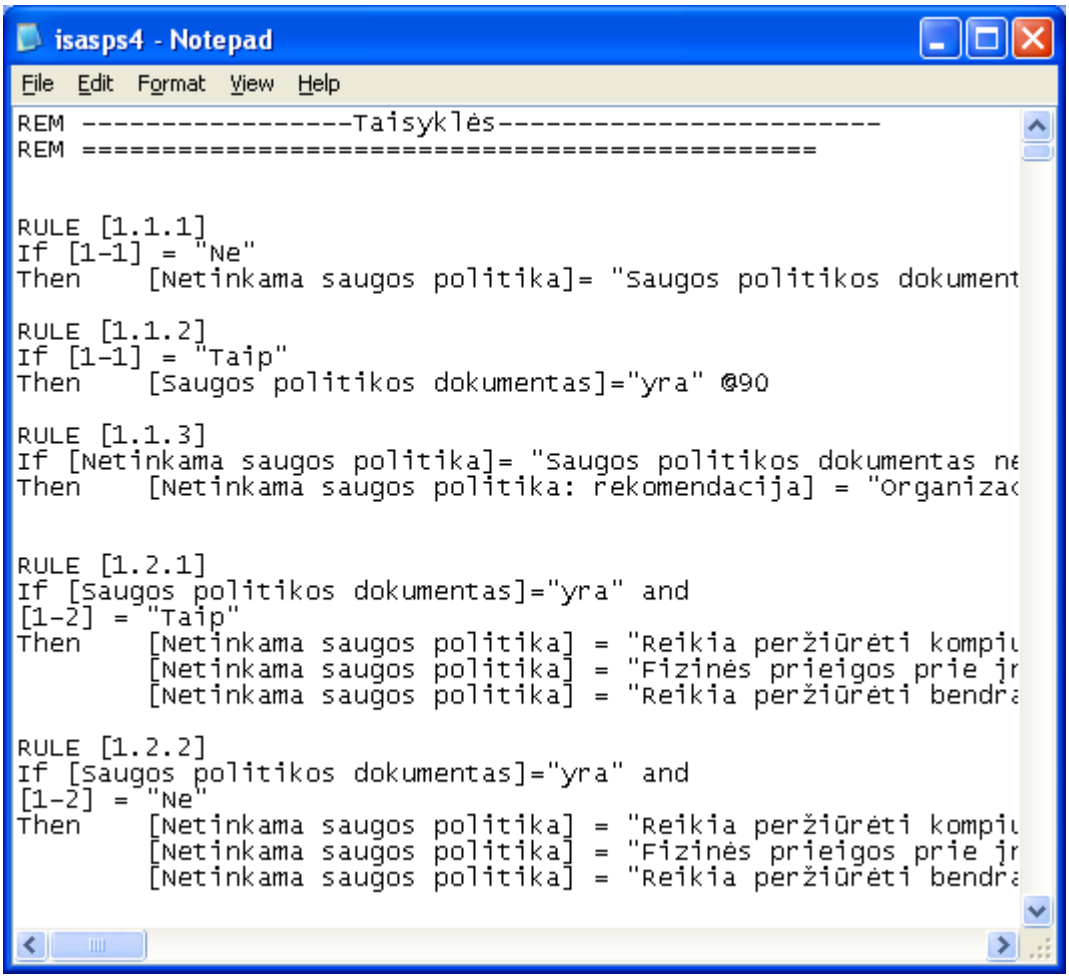
3. Žinių bazės analizės lange pateikiami atributų panaudojimai taisyklėse, atributo reikšmių panaudojimas taisyklėse ir išvadų panaudojimą taisyklėse.



25 pav. Atributių, atributų reikšmių ir išvadų panaudojimas taisyklėse

3.6.5. Informacijos saugos audito žinių bazės kūrimo aplinka

Žinių bazei, kuri naudoja neapibrėžtų faktų vertinimą, kurti nėra sukurtos grafinės vartotojo sąsajos. Tam reikia, naudojantis specialia e2glite sistemos kalba formuoti taisykles, pildyti klausimus ir rekomendacijas vienoje sistemos byloje, .kb tipo faile, kuris ir yra žinių bazė. Jis atidaromas su programa *Notepad*. Žinių bazės fragmentas pateiktas paveiksle 26.



26 pav. Žinių bazės kūrimo aplinka

3.6.6. Neapibrėžtų faktų valdymas realizuotoje sistemoje

Realizuota sistema naudoja pasitikėjimo faktorių metodą neapibrėžtų faktų valdymui. Pasitikėjimo faktorių galima reikšmių sritis yra nuo 0% iki 100%. 100% reiškia visišką pasitikėjimą, o 0% reiškia jokio pasitikėjimo.

Pasitikėjimo faktorių skaičiavimo algoritmai naudojami šiais atvejais:

- Pasitikėjimo faktoriai įvedami sistemos vartotojo;
- Pasitikėjimo faktoriai gaunami iš iškeltos taisyklės, susidedantys iš sąlygos pasitikėjimo laipsnio ir taisyklės pasitikėjimo laipsnio;

- Kombinuotas pasitikėjimo faktorius taisyklių, kurias sieja ta pati išvada;
- Bendras pasitikėjimas sprendimo paieškos grandinėje, kuris įtakoja išvadą.

1 pavyzdys. Vartotojo nurodyto pasitikėjimo vertinimas

Žemiau pateiktas pavyzdys yra sistemos teikiamas paaiškinimas rekomendacijos ”Organizacijai būtina parengti saugos politikos dokumentą”. Tam reikia patvirtinti dvi taisykles (1.1.3 ir 1.1.1).

Pirma buvo patvirtinta taisyklė 1.1.1. Kuri sako, kad “Saugos politikos dokumentas neegzistuoja” su 85% tikslumu, kai auditoriaus įvesta reikšmė yra „Ne“. O auditorius reikšmę „Ne“ įvedė su 80% tikslumu. Tuomet išvada „Saugos politikos dokumentas neegzistuoja“ yra teisingas 68% tikslumu, nes $\frac{80\% * 85\%}{100\%} = 68\%$. Analogiški skaičiavimai atliekami iš patvirtinti 1.1.3 taisyklę. Kadangi identifikuota „Saugos politikos dokumentas neegzistuoja“ su 68% tikslumu, tai rekomendacija yra “Organizacijai būtina parengti saugos politikos dokumentą” su 61,2% tikslumu, nes $\frac{68\% * 90\%}{100\%} = 61{,}2\%$

Nustatyta **Netinkama saugos politika: rekomendacija** yra **Organizacijai būtina parengti saugos politikos dokumentą** su 61.2% tikslumu iš:
Priskiriama CF=68.0% vertė išvadai **Organizacijai būtina parengti saugos politikos dokumentą** su 61.2% tikslumu:
Taisyklė: 1.1.3
Jeigu: Netinkama saugos politika reikšmė Saugos politikos dokumentas neegzistuoja
tai: Netinkama saugos politika: rekomendacija yra Organizacijai būtina parengti saugos politikos dokumentą (90.0%)
Nustatyta **Netinkama saugos politika** yra **Saugos politikos dokumentas neegzistuoja** su 68.0% tikslumu iš:
Priskiriama CF=80.0% vertė išvadai **Saugos politikos dokumentas neegzistuoja** su 68.0% tikslumu:
Taisyklė: 1.1.1
Jeigu: 1-1 reikšmė Ne
tai: Netinkama saugos politika yra Saugos politikos dokumentas neegzistuoja (85.0%)
Nustatyta **1-1** yra **Ne** su 80.0% tikslumu iš:
Ne Buvo įvesta 80.0% tikslumu

27 pav. Sistemos neapibrėžtumų vertinimas: vartotojo nurodyto pasitikėjimo vertinimas

2 pavyzdys. Tikimybinės sumos skaičiavimo panaudojimas

Žemiau pateiktas pavyzdys yra sistemos teikiamas paaiškinimas rekomendacijos ” Efektyviausia apsauga nuo slaptažodžių vagysčių ir kitokių atakų yra išmaniosios (Smart Cards) kortelės bei vienkartiniai slaptažodžiai. Vartotojas iš pradžių iš slaptažodžių generavimo sistemos gauna sąrašą skirtingų nenaudotų slaptažodžių, kurie galioja tik kartą.”. Tam reikia patvirtinti tris taisykles (4.1.3, 4.2.1 ir 4.3.1).

Kad taisyklė 4.3.1 būtų patvirtinta reikia patvirtinti sąlygą, t.y. „Vartotojai neteisingai naudoja slaptažodžius“. Ši sąlyga yra patvirtinama kitų dviejų taisyklių: 4.1.2, 4.2.1. Viena

taisyklė tą patvirtina su 45% tikslumu, o kita su 90% tikslumu. Kad gauti bendrą pasitikėjimą yra skaičiuojama tikimybinė suma 45.0% + 64.8% x (100% - 45.0%) = 80.64%.

Nustatyta **Netinkama prieigos kontrolė: rekomendacija** yra **Efektyviausia apsauga nuo slaptažodžių vagysčių ir kitokių atakų yra išmaniosios (Smart Cards) kortelės bei vienkartiniai slaptažodžiai. Vartotojas iš pradžių iš slaptažodžių generavimo sistemos gauna sąrašą skirtingų nenaudotų slaptažodžių, kurie galioja tik kartą.** su 64.512% tikslumu iš:

Priskiriama CF=80.64% vertė išvadai **Efektyviausia apsauga nuo slaptažodžių vagysčių ir kitokių atakų yra išmaniosios (Smart Cards) kortelės bei vienkartiniai slaptažodžiai. Vartotojas iš pradžių iš slaptažodžių generavimo sistemos gauna sąrašą skirtingų nenaudotų slaptažodžių, kurie galioja tik kartą.** su 64.512% tikslumu:
Taisyklė: 4.3.1
Jeigu: Netinkama prieigos kontrolė reikšmė Vartotojai neteisingai naudoja slaptažodžius
tai: Netinkama prieigos kontrolė: rekomendacija yra Efektyviausia apsauga nuo slaptažodžių vagysčių ir kitokių atakų yra išmaniosios (Smart Cards) kortelės bei vienkartiniai slaptažodžiai. Vartotojas iš pradžių iš slaptažodžių generavimo sistemos gauna sąrašą skirtingų nenaudotų slaptažodžių, kurie galioja tik kartą. (80.0%)
Nustatyta **Netinkama prieigos kontrolė** yra **Vartotojai neteisingai naudoja slaptažodžius** su 80.64% tikslumu iš:

Priskiriama CF=90.0% vertė išvadai **Vartotojai neteisingai naudoja slaptažodžius** su 45.0% tikslumu:
Taisyklė: 4.1.3
Jeigu: 4-1 reikšmė Ne visi
tai: Netinkama prieigos kontrolė yra Vartotojai neteisingai naudoja slaptažodžius (50.0%)
Nustatyta **4-1** yra **Ne visi** su 90.0% tikslumu iš:

Ne visi Buvo įvesta 90.0% tikslumu

Priskiriama CF=72.0% vertė išvadai **Vartotojai neteisingai naudoja slaptažodžius** su 64.8% tikslumu:
Taisyklė: 4.2.1
Jeigu: 4-2 reikšmė Taip ir
4-1 reikšmė Taip arba Ne visi
tai: Netinkama prieigos kontrolė yra Vartotojai neteisingai naudoja slaptažodžius (90.0%)
Nustatyta **4-2** yra **Taip** su 80.0% tikslumu iš:

Taip Buvo įvesta 80.0% tikslumu

Apskaičiuotas rekomendacijos pasitikėjimas srities Netinkama prieigos kontrolė yra Vartotojai neteisingai naudoja slaptažodžius: 45.0% + 64.8% x (100% - 45.0%) = 80.64%

28 pav. Sistemos neapibrėžtumų vertinimas: tikimybinės sumos skaičiavimas

3 pavyzdys. Skaičiavimas esant sudurtinėms sąlygoms

Žemiau pateiktas pavyzdys yra sistemos teikiamas paaiškinimas rekomendacijos ” Labai svarbu tinkamai išdėstyti užkardos taisykles: pradedant specialiomis ir baigiant bendrosiomis. Jose turi būti numatyta, kad išeinančio srauto paketų šaltinio adresai nesutaptų su išorinio tinklo adresais, o įeinančio – kad šaltinio adresai nesutaptų su vidinio tinklo adresais.”. Tam reikia patvirtinti dvi taisykles (4.9.1 ir 4.6.1).

Kad taisyklė 4.9.1 būtų patvirtinta reikia tenkinti tris sąlygas: patvirtinti išvadą „Netinkamai naudojamos ugniasienės“, ir surinkti iš auditoriaus žinias iš 4-8 ir 4-9 klausimų. Sąlyga „Netinkamai naudojamos ugniasienės“ yra patvirtinama taisyklės 4.6.1 su 72% tikslumu. 4-8 klausimo reikšmė gaunama „paketus filtruojančios užkardos“ su 100% tikslumu ir 4-9

klausimo reikšmė yra „Ne“ su 90% tikslumu. Tuomet apskaičiuojama vertė $\left(\frac{72\% * 100\%}{100\%}\right) * \frac{90\%}{100\%} = 58{,}32\%$.

Nustatyta **Netinkama prieigos kontrolė: rekomendacija** yra **Labai svarbu tinkamai išdėstyti užkardos taisykles: pradedant specialiomis ir baigiant bendrosiomis. Jose turi būti numatyta, kad išeinančio srauto paketų šaltinio adresai nesutaptų su išorinio tinklo adresais, o įeinančio – kad šaltinio adresai nesutaptų su vidinio tinklo adresais.** su 58.320004% tikslumu iš:

Priskiriama CF=64.8% vertė išvadai **Labai svarbu tinkamai išdėstyti užkardos taisykles: pradedant specialiomis ir baigiant bendrosiomis. Jose turi būti numatyta, kad išeinančio srauto paketų šaltinio adresai nesutaptų su išorinio tinklo adresais, o įeinančio – kad šaltinio adresai nesutaptų su vidinio tinklo adresais.** su 58.320004% tikslumu:
Taisyklė: 4.9.1
Jeigu: Netinkama prieigos kontrolė reikšmė Netinkamai naudojamos ugniasienės ir
4-8 reikšmė paketus filtruojančios užkardos ir
4-9 reikšmė Ne
tai: Netinkama prieigos kontrolė: rekomendacija yra Labai svarbu tinkamai išdėstyti užkardos taisykles: pradedant specialiomis ir baigiant bendrosiomis. Jose turi būti numatyta, kad išeinančio srauto paketų šaltinio adresai nesutaptų su išorinio tinklo adresais, o įeinančio – kad šaltinio adresai nesutaptų su vidinio tinklo adresais. (90.0%)
Nustatyta **Netinkama prieigos kontrolė** yra **Netinkamai naudojamos ugniasienės** su 72.0% tikslumu iš:

Priskiriama CF=90.0% vertė išvadai **Netinkamai naudojamos ugniasienės** su 72.0% tikslumu:
Taisyklė: 4.6.1
Jeigu: 4-6 reikšmė Ne ir
4-7 reikšmė Ne
tai: Netinkama prieigos kontrolė yra Netinkamai naudojamos ugniasienės (80.0%)
Nustatyta **4-6** yra **Ne** su 90.0% tikslumu iš:
Ne Buvo įvesta 90.0% tikslumu
Nustatyta **4-7** yra **Ne** su 100.0% tikslumu iš:
Ne buvo pateikta pagal nutylėjimą 100.0% tikslumu
Nustatyta **4-8** yra **paketus filtruojančios užkardos** su 100.0% tikslumu iš:
paketus filtruojančios užkardos Buvo įvesta 100.0% tikslumu
Nustatyta **4-9** yra **Ne** su 90.0% tikslumu iš:
Ne Buvo įvesta 90.0% tikslumu

29 pav. Sistemos neapibrėžtumų vertinimas: skaičiavimas esant sudurtinėms sąlygoms

Pastebėta, kad dauginimas yra naudojamas šiais atvejais:

- Kai taisyklės „If“ dalyje yra jungiamos kelios sąlygos jungtuku „and“.
- Kai taisyklės sąlyga yra kelių kitų taisyklių rezultatas.

3.7. Sistemos prototipo palyginimas su kitais IS audito programiniais įrankiai

Realizuotą sistemą palyginti su kitais panašiais programiniais įrankiais, skirtais informacijos saugos auditui, buvo keblu. Pirmiausia dėl to, kad nepavyko surasti sistemų, panašių savo funkcionalumu. Didžioji dalis įrankių yra daugiafunkciniai. Todėl lyginamos buvo tik tos savybės ir funkcijos, kurias turi realizuotas prototipas. Be to, sudėtinga kiekvieną įrankį ištirti, nes komerciniams tikslams skirtų sistemų kūrėjai pateikia tik sistemų aprašymus, daugumoje atveju nepavyko gauti net bandomųjų versijų.

Taip pat retai skelbiama informacija, kokius metodus naudoja sistemos rizikų vertinimui. Pavyko rasti, kad „Cobra“ ir „CRAMM“ naudoja ekspertinių sistemų priemones.

15 lentelė. Sistemos prototipo palyginimas su kitais IS audito programiniais įrankiais

	Cobra	**Security Decisions 2007**	**Callio Secura 17799**	**CounterMeasures**	**CRAMM**	**IS auditas**
Sprendimų/ rekomendacijų pateikimas	Taip	Taip	Ne	Taip	Taip	Taip
Rizikos vertinimas	Taip	Ne	Taip	Taip	Taip	Taip
Suderinamumas su standartais	ISO 17799	Ne	ISO 17799	NIST 800	ISO 27001	LST ISO/IEC 27001:2006
Neapibrėžtumų valdymas	Ne	Ne	Ne	Ne	Taip	Taip
Lietuvybės palaikymas	Ne	Ne	Ne	Ne	Ne	Taip
Paaiškinimų pateikimas	Ne	Ne	Taip	Ne	Ne	Taip
Grafinės ataskaitos pateikimas	Taip	Ne	Taip	Nežinoma	Taip	Ne
Dirba per interneto naršyklę	Ne	Ne	Ne	Ne	Ne	Taip

3.8. Sistemos prototipo kokybės įvertinimas

Sukurtos sistemos prototipo kokybę įvertinti padėjo nedidelės organizacijos padalinio vadovas. Darbuotojui, atlikusiam informacijos saugos auditą, buvo pateikta sistemos versija, bei kartu su juo buvo bandyta nustatyti:

- Sistemos vartotojo sąsajos paprastumą
- Rekomendacijų pateikimo tikslumą
- Pageidaujamų pakeitimų sąrašą

Atlikus informacijos saugos auditą vartotojas teigimai įvertino vartotojo sąsają, kuri yra paprasta ir nereikalauja jokio išankstinio pasiruošimo ar apmokymų. Be to, vartotojas liko patenkintas sistemos pasiekiamumu per interneto naršyklę. Norint naudotis sistema į kompiuterį nereikia diegti jokių papildomų programų. Informacijos saugos auditą atlikęs auditorius liko patenkintas ir pateiktų rekomendacijų detalumu. Tačiau rekomendacijų ir saugos spragų pateikimo formą reikėtų tobulinti: rezultatus pateikti lentelės forma ir grafiku, bei leisti išsaugoti atlikto audito rezultatus.

Tas pats darbuotojas, atlikęs žinių inžinieriaus rolę, pažymėjo, kad sistemos kūrimo aplinka nėra sudėtinga, tačiau butų paprasčiau naudotis specialia vartotojo sąsaja, skirta žinių pildymui. Tuomet būtų išvengta klaidų bei apsaugota žinių bazė nuo sugadinimo.

3.9. Išvados

Informacijos saugos audito sprendimų paramos sistemos kūrimui buvo apžvelgti 4 ekspertinių sistemų apvalkalai ir pasirinktas e2glite. Jis atitiko daugelį suprojektuotų reikalavimų:

- yra lengvai pasiekiamas iš bet kurios tinklo vietos, kur tik yra interneto prieiga, taigi jo nereikia diegti į kompiuterį;
- naudoja abu sprendimų paieškos metodus (tiesioginės ir atgalinės grandinės);
- žinioms aprašyti naudoja taisykles;
- gali vertinti neraiškias žinias, tam naudodamas pasitikėjimo faktorių metodu;
- yra nemokama.

Pasinaudojant ekspertinių sistemų apvalkalu e2glite buvo sukurta informacijos saugos audito sprendimų paramos sistema. Sistema talpina žinių bazę, kuri suformuota remiantis informacijos saugos standartu LST ISO/IEC 27001:2006. Realizuota žinių bazė apima kompiuterių tinklų saugą, kuri paremta standarto išskirtomis 5 (iš 11) sričių:

- Saugumo politika
- Fizinė ir aplinkos sauga
- Komunikacinių kanalų ir procesų valdymas
- Prieigos kontrolė
- Personalo sauga

Realizuotoje sistemoje galimos dvi vartotojų rolės: informacijos saugos auditorius neprofesionalas ir informacijos saugos ekspertas.

Atlikus realizuotos sistemos prototipo neapibrėžtumų valdymo tyrimą paaiškėjo, kad sistema naudoja du neapibrėžtų faktų vertinimo būdus: dauginimą ir tikimybinę sumą. Projektavimo dalyje buvo apsibrėžta naudoti 5 pasitikėjimo faktorių skaičiavimo metodus: minimalus, maksimalus, vidurkis, tikimybinė suma ir dauginimas. Sudurtinėms taisyklėms naudojant minimalų, maksimalų ir vidurkio metodą būtų galima gauti dar tikslesnius rezultatus.

Realizuotoje sistemoje rekomendacijos pateikiamos tekstine forma, dėl to informacijos saugos auditoriui neprofesionalui yra nelabai patogios.

Realizuota sistema sprendimų paieškai naudoja kombinuotą metodą: apjungtą tiesioginės ir atgalinės grandinės metodą.

Sistemos prototipas buvo palygintas su kitomis informacijos saugos auditui skirtomis automatizuotomis sistemomis, bei atliktas kokybės įvertinimas.

Būtina paminėti, kad realizuota sistema neturi tokių galimybių, kaip istorijos kaupimas, saugojimas, audito rezultatų palyginimas, grafinis rezultatų atvaizdavimas, žinių bazės kūrimo vartotojo sąsajos. Visus šiuos komponentus, esant poreikiui, galima būtų realizuoti.

IŠVADOS

Informacijos saugos audito metodų ir priemonių analizės dalyje buvo išanalizuota informacijos saugos audito problema, aprašyta audito procedūra, informacijos saugos audito automatizavimo priemonės. Apžvelgti ir palyginti su informacijos sauga susiję standartai, bei išskirti standartai oficialiai pripažinti ir galiojantys Lietuvoje. Atlikus pasaulinėje rinkoje esamų priemonių, skirtų IS auditui analizę, paaiškėjo, kad nėra sistemos, pritaikytos Lietuvos rinkai, bei skirtos kitam rinkos segmentui.

Nustatyta, kad reikalingos tokios priemonės, kurių pagalba auditą galėtų nesudėtingai atlikti neprofesionalas, t.y. organizacijos darbuotojas, atsakingas už informacijos saugą, bei visam vadovaujančiam personalui, neturinčiam specifinių techninių saugos arba auditavimo žinių, bet galintiems prieiti prie svarbios informacijos.

Darbe buvo iškeltas tikslas – sukurti informacijos saugos audito paramos sistemą, kuri palengvintų priimti sprendimus ir pateiktų rekomendacijas informacijos saugai sustiprinti. Sistema turi padėti nustatyti rizikos faktorius pagal LST ISO/IEC 27001:2006 standarto reikalavimus ir pasiūlyti rekomendacijas saugumo didinimui.

Išanalizavus sprendimų paramos sistemų galimybes paaiškėjo, kad tokios sistemos tinkamos IS audito problemai spręsti dėl savybės imituoti žmogaus sprendimų priėmimo sugebėjimus.

Projektavimo dalyje buvo sudarytas informacijos saugos sprendimų paramos sistemos modelis. Sistema suprojektuota taip, kad galėtų vertinti neapibrėžtus faktus, tam naudodama pasitikėjimo faktorių metodą.

Teigiama, kad magistro darbo tikslas pasiektas:

- Sistemoje galimos dvi vartotojo rolės: informacijos saugos auditorius neprofesionalas, ir informacijos saugos ekspertas. Todėl auditą gali atlikti neprofesionalas, taip sumažinant kaštus. Informacijos saugos ekspertas nesudėtingai gali plėsti žinių bazę, t.y. sistema lengvai tobulinama, bei pritaikoma kintančioje aplinkoje.
- Sistemos žinių bazė sudaryta taip, kad būtų galima atlikti rizikos vertinimą pagal LST ISO/IEC 27001:2006 standartą, bei, identifikavus konkrečias saugumo sritis, pateiktų detalias rekomendacijas informacijos saugai gerinti;
- Sistema gali vertinti neapibrėžtus faktus, naudodama pasitikėjimo faktorių metodą, dėl to pasižymi savo pateikiamų rekomendacijų tikslumu;

- Atlikus programinių įrankių analizę, buvo nustatyta, kad daugelis informacijos saugos auditui skirtų programų turi būti diegiamos į kompiuterį, be galimybės pasiekti sistemą iš bet kurios tinklo vietos per interneto naršyklę. Todėl prototipo realizavimui buvo pasirinkta e2glite ekspertinių sistemų apvalkalas, kuris parašytas java kalba ir yra įterpiamas į interneto naršyklę. Be to, tik viena palyginta sistema naudoja neapibrėžtų žinių vertinimą.
- Atlikus realizuotos sistemos prototipo neapibrėžtumų vertinimo tyrimą paaiškėjo, kad sistema naudoja du neapibrėžtų faktų vertinimo būdus: dauginimą ir tikimybinę sumą. Projektavimo dalyje buvo apsibrėžta naudoti 5 pasitikėjimo faktorių skaičiavimo metodus: minimalus, maksimalus, vidurkis, tikimybinė suma ir dauginimas. Sudurtinėms taisyklėms naudojant minimalų, maksimalų ir vidurkio metodą būtų galima gauti dar tikslesnius rezultatus.
- Įvertinus sistemos prototipo kokybę kaip teigiamos sistemos savybės buvo pažymėtos: vartotojo sąsajos paprastumas, nereikalauja diegti į vartotojo kompiuterį jokių programų, pateikiamų rekomendacijų detalumas. Kaip trūkumai buvo paminėti: rezultatų pateikimas tik tekstine forma, žinių bazės inžinieriui nėra sukurtos grafinės aplinkos žinių bazės pildymui.
- Informacijos saugos auditui atlikti naudojama sukurta patogi vartotojo aplinka. Bet sistemos prototipas neturi vartotojo sąsajos, skirtos ekspertui, žinių bazės pildymui, todėl jam reikia išmanyti žinių aprašymo kalbą. Ji nėra sudėtinga, bet reikalauja minimalių apmokymų. Esant poreikiui ir plečiant sistemą galima sukurti vartotojo sąsają, skirtą informacijos saugos ekspertui.

LITERATŪRA

[1] AMS9000 [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą: http://www.noweco.com/smhe.htm.

[2] Babeanu, D.; Mares, V. Standards Review on Mission of Management Information Systems Audit, Journal of Applied Quantitative Methods, 2009.

[3] Baskerville, R. The Information Security Standards Marketplace, 17th Australasian Conference on Information Systems, 2006.

[4] Building and Using Expert Systems: a Mini-Course Introducing the e2gLite Expert System Shell [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą: http://www.expertise2go.com/webesie/e2gdoc/e2gmod1.htm.

[5] Callio Secura 17788 [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą: http://www.callio.com/PDF/Calio_Secura17799.pdf.

[6] Clips – A Tool for Building Expert Systems [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą: http://clipsrules.sourceforge.net/index.html .

[7] Cobit [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą: www.isaca.org/cobit/.

[8] COBRA [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą: http://www.riskworld.net/.

[9] De Kock, E Chapter 2 – Knowledge-based Decision Support Systems, University of Pretoria etd., Anglija, Londonas, 2003.

[10] Dwivedi, A.; Mishra, D.; Klara, P. K. Handling Uncertainties – using Probability Theory to Possibility Theory. The Magazine of IIT Kanpur, Volume 7 Number 3, 2006. [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą: http://www.iitk.ac.in/directions/feb2006/.

[11] Dzemydienė, D. *Intelektualizuotų informacinių sistemų projektavimas ir taikymai*. Vilnius, 2006, p. 185-237, ISBN 9955-19-051-5.

[12] Eom, Sean B.; Decision Support Systems: International Encyclopedia of Business and Management, 2nd Edition, International Thomson Business Publishing Co., 2001.

[13] FuzzyCLIPS Version 6.10d User's Guide [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą:http://moxie.oswego.edu/doc/clips/FuzzyCLIPS.pdf .

[14] Galimybių teorija, [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą: http://en.wikipedia.org/wiki/Possibility_theory .

[15] Henczel, S. The Information Audit As a First Step Towards Effective Knowledge Management: An Opportunity for the Special Librarian, Inspel 34, 2000, p. 210-226.

[16] Information Security Audit, *Training for Information Processing Oginawa Internationa, Centre Japan International Cooperation Agency*, 2006, CNS03E06A.

[17] Information Security Audit (IS audit) - A guideline for IS audits based on IT-Grundschutz [interaktyvus], 2008 [žiūrėta 2010-05-17]. Prieiga per internetą:

https://www.bsi.bund.de/cae/servlet/contentblob/471376/publicationFile/27987/guideline-isrevision_pdf.pdf

[18] ISF Standart of Good Practise for Information Security [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą: https://www.isfsecuritystandard.com.

[19] ISO IEC 27002 (17799) Information Security Management Library [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą: http://www.praxiom.com/.

[20] IT apsauga Lietuvoje [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą: http://www.esecurity.lt/info.php?ident=it&type_id=.

[21] IT Audit Guidelines: 6th ASOSAI Research Project, 2003, p. 2-3, p. 80-81.

[22] Įsakymas dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=233268&p_query=informacijos%20technologij%F8%20saugos&p_tr2=1.

[23] Jess – the Rule Engine for the Java™ Platform [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą: http://www.jessrules.com/ .

[24] Lietuvos standartizacijos departamentas. Lietuvos sertifikatas [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą: http://www.lsd.lt/standards/test.php?s=17799&reference=&nuo=&iki=&del_nuo=&del_iki=&ics=&direktyva=&tk=&del=&go=Paie%F0ka.

[25] Mandol, P. S.; Verma, M. Formulation of IT Auditing Standards, IT Audit Seminar organized by National Audit Office, 2004, 2 p.

[26] Merkevičius, E.; Garšva, G.; Cepkovaja, O. Intelektualios sprendimų paramos sistemos struktūra kredito rizikos vertinimui, *Informacinių sistemų projektavimo metodai ir technologijos*, 2005.

[27] NIST SP800 [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą: http://csrc.nist.gov/publications/PubsSPs.html.

[28] Nutarimas dėl duomenų apsaugos valstybės ir vietos savivaldos informacinėse sistemos [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=42817&p_query=&p_tr2= .

[29] Power, D.J. *A* Brief History of Decision support systems. Decision support systems resources [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą: http://dssresources.com/history/dsshistory.html.

[30] SANS Institute InfoSec Reading Room, The Application Audit Process - A Guide for Information Security Professionals [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą: http://www.sans.org/.

[31] Security Decisions 2007 [interaktyvus], [žiūrėta 2010-05-17]. Prieiga per internetą: http://manalytic.com/SW/SD-Drill-Down.html.

[32] University of Manitoba, Comp 4200 Expert Systems paskaitų medžiaga [interaktyvus], 2007 [žiūrėta 2010-05-17]. Prieiga per internetą: http://www.cs.umanitoba.ca/~comp4200/

[33] Venčkauskas, A.; Kazanavičius, E.; Liutkevičius, A. *Informacijos saugos vadyba*. Kaunas, 2008, p. 142-146.
[34] Yang, Jian-Bo; Liu, J.; Wang, Jin. Belief Rule-Base Inference Methodology Using the Evidential Reasoning Approach – Rimer. IEEE Transactions on Systems, Man, and Cybernetics. Part A: System and Humans, Vol. 36, No.2 March 2006.
[35] ZHU, X.; HEALEY, R. G.; ASPINALL, R. J. A Knowledge-Based Systems Approach to Design of Spatial Decision Support Systems for Environmental Management. Environmental Management Vol. 22, No. 1, 1998, p. 35–48.