VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

FUNDAMENTINIŲ MOKSLŲ FAKULTETAS

INFORMACINIŲ SISTEMŲ KATEDRA

Vitalijus Gurčinas

EKSPERTINIŲ SISTEMŲ TAIKYMO INFORMACIJOS SAUGOS VALDYMO PROCESE TYRIMAS

STUDY OF EXPERT SYSTEMS USE IN THE INFORMATION SECURITY MANAGEMENT PROCESS

Baigiamasis magistro darbas

Informacijos ir informacinių technologijų saugos studijų programa, valstybinis kodas 621E14007

Informatikos inžinerijos studijų kryptis

Vilnius, 2014

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

FUNDAMENTINIŲ MOKSLŲ FAKULTETAS

INFORMACINIŲ SISTEMŲ KATEDRA

TVIRTINU
Katedros vedėjas

_____
(Parašas)

_____
(Vardas, pavardė)

_____
(Data)

Vitalijus Gurčinas

EKSPERTINIŲ SISTEMŲ TAIKYMO INFORMACIJOS SAUGOS VALDYMO PROCESE TYRIMAS

STUDY OF EXPERT SYSTEMS USE IN THE INFORMATION SECURITY MANAGEMENT PROCESS

Baigiamasis magistro darbas

Informacijos ir informacinių technologijų saugos studijų programa, valstybinis kodas 621E14007

Informatikos inžinerijos studijų kryptis

Vadovas _____ _____ _____
(Moksl. laipsnis/pedag. vardas, vardas, pavardė) (Parašas) (Data)

Konsultantas _____ _____ _____
(Moksl. laipsnis/pedag. vardas, vardas, pavardė) (Parašas) (Data)

Konsultantas _____ _____ _____
(Moksl. laipsnis/pedag. vardas, vardas, pavardė) (Parašas) (Data)

Lietuvių kalbos konsultantas _____ _____ _____
(Moksl. laipsnis/pedag. vardas, vardas, pavardė) (Parašas) (Data)

Vilnius, 2014

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
FUNDAMENTINIŲ MOKSLŲ FAKULTETAS
INFORMACINIŲ SISTEMŲ KATEDRA

TVIRTINU
Katedros vedėjas

_____
(Parašas)

_____
(Vardas, pavardė)

_____
(Data)

Informatikos inžinerijos studijų kryptis

Informacijos ir informacinių technologijų saugos studijų programa, valstybinis kodas 621E14007

BAIGIAMOJO MAGISTRO DARBO UŽDUOTIS

…….....Nr. .....
Vilnius

Studentui (ei) .....Vitalijui Gurčinui…….....….....….....….....
(Vardas, pavardė)

Baigiamojo darbo tema: .....…Ekspertinių sistemų taikymo informacijos saugos valdymo procese tyrimas.....
.....

patvirtinta 201…m. ……..…… d. dekano potvarkiu Nr. …….

Baigiamojo darbo užbaigimo terminas 201…m. ……..…… d.

BAIGIAMOJO DARBO UŽDUOTIS:

...Išanalizuoti ekspertinių sistemų taikymą įmonių informacijos saugos valdymo procese. Sukurti ekspertinę sistemą orientuotą į smulkios arba vidutinės įmonės rizikos analizės procesą (su galimybe adaptuotis prie įmonės tipo, aplinkos ir kt.) ir išbandyti sistemą eksperimentiškai.
.....
.....

Baigiamojo darbo rengimo konsultantai:
…….
…….....
.....
.....
(Moksl. laipsnis/pedag. vardas, vardas, pavardė)

Vadovas ....doc. dr. Nikolaj Goranin.....
(Parašas) (Moksl. laipsnis/pedag.vardas, vardas, pavardė)

Užduotį gavau

……..
(Parašas)
…Vitalijus Gurčinas……...…..
(Vardas, pavardė)
……2012.10.03...……..…....
(Data)

Vilniaus Gedimino technikos universitetas
Fundamentinių mokslų fakultetas
Informacinių sistemų katedra

ISBN ISSN
Egz. sk. .....
Data .....-.....-.....

Antrosios pakopos studijų **Informacijos ir informacinių technologijų saugos** programos magistro baigiamasis darbas

Pavadinimas **Ekspertinių sistemų taikymo informacijos valdymo procese tyrimas.**

Autorius **Vitalijus Gurčinas**

Vadovas **doc. dr. Nikolaj Goranin**

Kalba: lietuvių

Anotacija

Darbe analizuojama ekspertinių sistemų taikymas įmonių informacijos saugos valdymui ir pateikiamas ekspertinės sistemos modelis, skirtas smulkios arba vidutinės įmonės rizikos analizės procesui. Analitinėje dalyje pateikiama ekspertinių sistemų analizė: veikimo principas, privalumai, trūkumai, architektūros tipai, žinių ir duomenų bazės pildymas, esamos ekspertinės sistemos taikomos infomacijos saugos valdymui, ekspertinių sistemų taikymas gretutinėse srityse, integracijos galimybės. Išanalizuoti ES kūrimo įrankiai ir pasirinktas įrankis ES modelio kūrimui. Praktinėje dalyje pateikiamas ekspertinės sistemos projektas, taikomas rizikos analizės mechanizmas, jos vertinimo pagrindas, ekspertinės sistemos testavimo būdai. Eksperimentinėje dalyje yra lyginamos ir analizuojamos sistemos išvados su realių ekspertų išvadomis, gautomis atlikus apklausą. Darbą sudaro šešios dalys: Įvadas; analitinė dalis; praktinė dalis; eksperimentas; išvados ir darbo rezultatai; literatūra. Darbo apimtis – 70 p. teksto, 11 pav., 8 lent., 44 bibliografinių šaltinių, 2 priedai.

Prasminiai žodžiai: ekspertinė sistema, informacijos sauga, vidutinio dydžio įmonė, saugos valdymas, informacijos saugos rizika, taisyklėmis pagrįsta ekspertinė sistema.

Vilnius Gediminas Technical University
Faculty of Fundamental Sciences
Department of Information Systems

ISBN ISSN
Copies No. .....
Date .....-.....-.....

Master Degree Studies **Information and Information Technologies Security** study programme
Master Graduation Thesis

Title **Study of expert systems use in the information security management process**

Author **Vitalijus Gurčinas**

Academic supervisor **Assoc Prof Dr Nikolaj Goranin**

Thesis language:
Lithuanian

Annotation

The thesis analyzes expert systems use in enterprise information security management process and presents expert system model oriented on small and medium enterprise risk analysis process. Analytic part of the work provides analysis of the expert systems: principle of functioning, advantages and disadvantages, architectural types, knowledge and data base filling, existing expert systems used for information security management, expert systems use in adjacent areas, integration capabilities. Expert system development tools are analyzed and selection of appropriate tool for expert system build is chosen. Practical part of the work provides expert system project, used risk analysis mechanism, basis of assessment work, expert system testing methods. The experimental part provides data analysis of expert system and results comparison with real experts findings based on the survey. Thesis consists of six parts: an introduction, analytical part, practical part, experiment, conclusions and results of the work, references. Size of work - 70 p. text, 11 figures., 8 tables., 44 bibliographic sources, 2 appendices.

Keywords: expert system, information security, medium-size enterprise, security management, information security risk, rule-based expert system.

Vilniaus Gedimino technikos universiteto egzaminų, sesijų ir baigiamųjų darbų rengimo bei gynimo organizavimo tvarkos aprašo 2011-2012 m. m.

1 priedas

(Baigiamojo darbo sąžiningumo deklaracijos forma)

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Vitalijus Gurčinas,

(Studento vardas ir pavardė, studento pažymėjimo Nr.)

Fundamentinių mokslų fakultetas

(Fakultetas)

Informacijos ir informacinių technologijų sauga, ITSfm-12

(Studijų programa, akademinė grupė)

BAIGIAMOJO DARBO (PROJEKTO) SĄŽININGUMO DEKLARACIJA

2014 m. gegužės 27 d.

Patvirtinu, kad mano baigiamasis darbas tema „Ekspertinių sistemų taikymo informacijos valdymo procese tyrimas" patvirtintas 2013 m. spalio 28 d. dekano potvarkiu Nr. 371fm, yra savarankiškai parašytas. Šiame darbe pateikta medžiaga nėra plagijuota. Tiesiogiai ar netiesiogiai panaudotos kitų šaltinių citatos pažymėtos literatūros nuorodose.

Mano darbo vadovas doc. dr. Nikolaj Goranin.

Kitų asmenų indėlio į parengtą baigiamąjį darbą nėra. Jokių įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs (-usi).

(Parašas)

Vitalijus Gurčinas

(Vardas ir pavardė)

Turinys

Santrumpos

AHP – analitinis hierarchinis procesas (angl. *Analytic Hierarchy Process*)

AI – dirbtinis intelektas (angl. *Artificial Intelligence*)

CLI – komandinės eilutės aplinka (angl. *Command-line interface*)

DoS – atsisakymas aptarnauti (angl. *Denial of Service*)

DSS – sprendimų priėmimo sistema (angl. *Decision Support System*)

EC – elektroninė komercija (angl. *Electronic Commerce*)

ES – ekspertinė sistema (angl. *Expert System)*

ESE – ekspertinės sistemos aplinka (angl. *Expert System Environment*)

IS – informacinė sistema (angl. *Information System*)

ISO – tarptautinė standartizacijos organizacija (angl. *International Organization for Standardization*)

IT – informacinės technologijos (angl. *Information Technology*)

MCDM – sprendimų priėmimas pagal keletą kriterijų (angl. *Multi Criteria Decision Making*)

(N)IDES – (tinklo) įsilaužimo aptikimo ekspertinė sistema (angl. *(Network) Intrusion Detection Expert System*).

RACF – išteklių prieigos kontrolės įranga (angl. *Resource Access Control Facility*)

XML – praplečiamoji dokumentų aprašų kalba (angl. *Extensible Markup Language*)

Paveikslų sąrašas

Lentelių sąrašas

Įvadas

Darbo aktualumas

Informacijos saugumas tampa vis svarbesniu klausimu kiekvienam informacijos turėtojui ir jos naudotojui. Įmonių savininkams ir vadovams informacijos saugos klausimas - ne išimtis. Dabartiniame technologijų amžiuje didelė dalis įmonės veiklos remiasi vidaus ir išorės kompiuterinėmis, valdymo, ryšio sistemomis, tad negali sau leisti turėti bet kokių jų veiklos sutrikimų, susijusių su informacijos konfidencialumu, prieinamumu ir integralumu. Iškilę saugos incidentai gali turėti plataus masto neigiamą poveikį įmonės pajamoms, prestižui, klientų pasitikėjimui. Ši dilema padaro informacijos saugą viena iš esminių efektyvaus verslo strategijos sudedamųjų dalių. Todėl reikalinga sukurti, įgyvendinti ir valdyti informacijos saugos politiką, kuri padėtų išsiaiškinti, prioritetizuoti ir mažinti rizikas, su kuriomis verslas susiduria.

Net ir pats mažiausias šiuolaikinis verslo vienetas turi informacijos ir IS, kurias privalu saugoti. IS sudarančių vienetų ir versle naudojamos techninės įrangos skaičiams sparčiai augant, tuo pačiu metu atitinkamai didėja ir galimų pažaidų kiekiai, kurie apima tiek organizacinę, tiek techninę įmonės pusę. Informacijos saugos valdymas tampa svarbiu uždaviniu net mažose ar vidutinėse įmonėse, kadangi duomenys, dokumentai, pats verslas tampa visiškai elektroninis ir priklausomas nuo informacijos ir jos valdymo sistemų. Taip pat ir informacijos sauga plečia savo ribas, reikalaudama specialių žinių patvirtinant ar paneigiant iškeltą hipotezę, tikėtiną rizikos laipsnį. Ne specialistui įvertinti visas grėsmes ir rizikas be papildomų priemonių yra, galima sakyti, neįmanoma. Tačiau pastebima tendencija, jog kuo verslo subjektas yra mažesnis, tuo yra didesnė tikimybė, kad organizacija neturi ar galvoja, kad yra nereikalinga ne tik atskiras kompetentingas asmuo, kuris būtų atsakingas už informacijos saugos valdymą, jos vykdymo politiką, grėsmių ir rizikos įvertinimą, bet ir bendrų informacijos saugos metodų taikymą.

Būtent dėl šių priežasčių iš pažiūros maža problema gali tapti esmine visos įmonės mastu, įvykus nepageidaujamiems įvykiams, tokiems kaip informacijos atskleidimas, neteisėtas panaudojimas, modifikavimas ar net sunaikinimas. Tai ypač pastebima mažose arba vidutinėse įmonėse dėl aukščiau aptarto vadovų supratimo ir požiūrio į informacijos saugą. Todėl atsiranda poreikis turėti įrankį, kuriuo įmonės darbuotojai galėtų atlikti informacijos saugos valdymo funkcijas.

Darbo naujumas

Verslo subjekto savininkams ar vadovams yra aiški verslo ir techninio požiūrio integracija, bet dažnai yra klaidingai vertinama, jog sauga yra didinama, įgijus papildomų techninių ar programinių priemonių. Papildomos priemonės iš esmės nėra brangios, nereikalauja atitinkamo personalo ir jų

pagrindu dažnai galima užtikrinti priimtiną saugos valdymo lygį, bet visada reikia įvertinti konkrečią jų įsigijimo naudą, kas beveik niekada nedaroma mažose ir vidutinėse įmonėse.

Visa kas paminėta, tai tik dalis ar netiesioginis informacijos saugos požiūris į riziką, kadangi rizikos įvertinimo procesas yra sudėtingesnis nei "taip" arba "ne", reikalaujantis išsamaus visos sistemos supratimo, galintis įvertinti informacijos saugos sąnaudas, alternatyvų galimybes ir nustatyti geriausiai tinkančius metodus ir priemones, remiantis rizikos apskaičiavimu. Tai gali atlikti tik informacijos saugos ekspertas ar profesionalas. Todėl iškyla klausimas, kaip apsaugoti informaciją ir IS nuo nepageidaujamų įvykių ir veiksnių, keliančių grėsmę turtui, nesant saugos specialistui įmonėje. Kaip vienas iš galimų sprendimo būdų šiai aktualiai problemai spręsti, yra pasinaudoti ekspertine sistema, apie kurios pritaikymą saugos valdymui iki šiol tik diskutuota ar pateiktas tik teorinis siauros srities modelis.

Darbo tikslas

Šio darbo tikslas - pasiūlyti ekspertinės sistemos modelį, skirtą smulkios arba vidutinės įmonės informacijos saugos rizikos analizei.

Darbo tikslui pasiekti darbe reikia spręsti šiuos uždavinius:

1. Išanalizuoti esamas savarankiškas ir integruotos ES į įmonių verslo valdymo (analitikos) sistemas, kurios taikomos įmonių informacijos saugos valdymo procese.
2. Išanalizuoti ES, taikomas kitose srityse.
3. Sukurti ES modelio koncepciją, skirtą smulkios arba vidutinės įmonės rizikos analizės procesui, kuri taip pat adaptuotųsi prie įmonės tipo, aplinkos ir kitų parametrų.
4. Realizuoti pasiūlytą ES modelį.
5. Sistemą išbandyti eksperimentiškai.

Taikyti tyrimų metodai

Darbe naudojamas teorinis ir empirinis tyrimo metodai. Teorinio tyrimo metu yra analizuojami mokslinės literatūros šaltiniai, peržiūrima antriniuose ir tretiniuose šaltiniuose pateikiami susiję duomenys. Empirinio tyrimo metu yra atliekamas kiekybinis ekspertinės sistemos validacijos eksperimentas, apdorojami ir įvertinami gauti eksperimento duomenys.

Mokslinė vertė

Pasiūlytame ekspertinės sistemos modelyje yra taikoma keletas rinktinių sprendimų, kurie aprašyti teoriniuose šaltiniuose. Taip pat pasiūlytas sprendimas parodo galimybę rizikos analizei taikyti

aktualius dabartinius faktus iš dinaminės faktų bibliotekos, kurie daro pasiūlytą ekspertinę sistemą ne vienadiene.

Darbo praktinė vertė

Iki šiol nei ekspertinių sistemų piko metu, nei vėlesniais metais atskiros ekspertinės sistemos, plačiai apimančios informacijos saugos valdymą, sukurta nebuvo. Šiuo metu ES, skirtos informacijos saugos valdymui, egzistuoja tik integruotos į įmonių valdymo sistemas, kurios yra pritaikytos tos įmonės veiklos sričiai. Galima rasti ir klausimyno tipo tariamąsias ES, skirtas bendriems informacijos saugos valdymo taikymams, kas faktiškai yra ne kas kita, kaip tam tikrų saugos standartų realizacija klausimų ir atsakymų principu.

Darbe pasiūlytas ekspertinės sistemos modelis gali būti taikomas tiek tiesiogiai, tiek netiesiogiai informacijos saugos valdymui. Netiesiogiai gali būti taikomas, kai norima išsiaiškinti tikėtinos rizikos padidėjimą, kintant IT infrastruktūrai ar informacijos valdymo procesams.

1. ES ir jų taikymo informacijos saugos srityje analizė

Analizuojama literatūra apie ES sistemas ir jų taikymą nėra nauja. Tą lėmė kelios priežastys. Šio amžiaus literatūroje ES ir jų veikimo metodai aprašomi abstrakčiai, daugiau gilinantis į sistemos rezultatus, o ne į veikimo principus, kai praeito amžiaus literatūros šaltiniuose, pradedant nuo pirmųjų ES sukūrimo, viskas aprašoma tiksliai, pradedant terminais ir baigiant vartota programavimo kalba. Taip pat pačioje naujausioje literatūroje pastebėtas dėmesys ES integracijai į įvairias sistemas, srities ontologijų panaudojimą, tačiau mažiau ir abstrakčiau kalbant apie pačią ES, kurios vis tiek yra kurtos senesniųjų ES kartų pagrindu.

1.1. Ekspertinių sistemų analizė

AI sistema, sukurta konkrečios probleminės srities uždavinių sprendimui, vadinama ekspertine sistema. Žinių, reikalingų ekspertinės sistemos papildymui, šaltinis - atitinkamos srities ekspertai [23]. Ekspertinė sistema ir yra pirmoji AI mokslinių tyrimų srities įgyvendinimas programinėje įrangoje. Taikomosios programinės įrangos kūrėjams, ypač besispecializuojantiems medicinos ir inžinerinių mokslų srityje, tai padėjo realizuoti sprendimų priėmimo procesą panaudojant simbolines, o ne skaitines reikšmes [22]. Tačiau yra ir kitoks požiūris, pagal kurį ES sistema turi ekspertų taisykles ir vengia aklos paieškos, motyvuoja pagal manipuliuojamus simbolius, supranta pagrindinius srities principus ir turi paprastesnius argumentavimo metodus, kai ekspertų taisyklės nebetinka, bei juos panaudoja motyvui paaiškinti. ES yra susijusi su sudėtingomis problemomis kompleksiškoje srityje, gali nustatytu metodu pateiktą problemą konvertuoti į vidiniam panaudojimui skirtą tipą apdorojimui su ekspertų taisyklėmis, ir jį gali argumentuoti turimomis žiniomis ar jų dalimi, ypač racionaliai atkurti pateiktos išvados priėmimo būdą paaiškinimams ir pagrindimams [8]. Taigi pagrindinė ES funkcija yra imituoti patirtį ir platinti ekspertų žinias ne ekspertams.

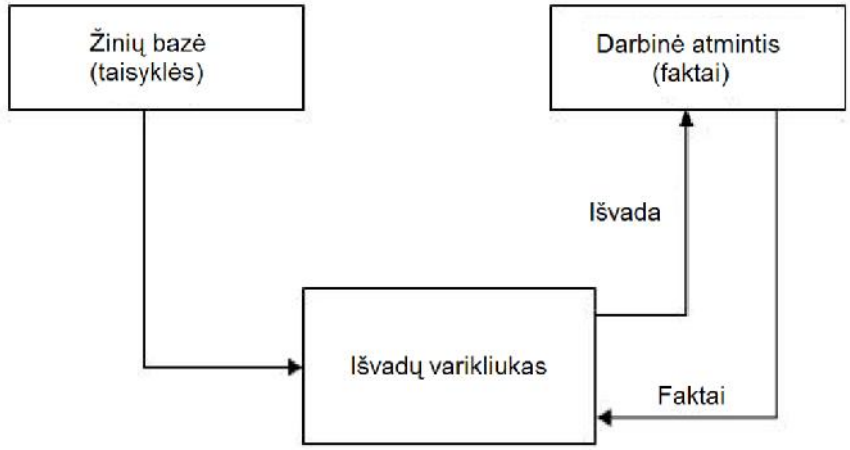
1.1.1. ES raida

Pirmieji straipsniai apie ES pasirodė 1970-ųjų metų pabaigoje ir labai greitai išpopuliarėjo žurnaluose, konferencijose, knygose 1980-ųjų pradžioje. Tą galima pastebėti ir dabar, kadangi didelė dalis literatūros apie ES remiasi ir cituoja būtent tų laikų literatūrą. Po 2000-ųjų metų literatūros šia tema ženkliai sumažėjo, kadangi ES tapo galimos ne vien panaudojant specifines ES aplinkas, o ir integruojant ES į taikomąsias programas ar tik ES sistemų išvadų varikliuko panaudojimui tam tikriems tikslams.

Pirmosios dvi dažniausiai eskaluotos ES, kitaip dar vadintos žiniomis pagrįstomis ES, buvo MYCIN ir DENDRAL, kurios leido sistema susidomėjusioms pusėms pažvelgti ir į ES vidų [22]. Jau minėtos ir vėlesnes ekspertinės sistemos buvo įvardijamos kaip kompiuterinės programos turinčios AI,

skirtos emuliuoti eksperto mąstymą ir jo struktūrą, turinčios eksperto gebėjimų ir įgūdžių, kuriais galėtų pasinaudoti ne ekspertas [41]. Toks apibrėžimas patiko ne visiems, todėl atsirado teigiančių, jog ES nenusipelno AI vardo dėl jos negalėjimo mokytis ir remtis patirtimi, kad gerintų rezultatus [39]. Kiti atkakliai teigė, jog sistema, turinti AI, laikoma tik ta, kuri gali išlaikyti Turingo testą [38].

Vėlesniųjų ES raidos laikotarpiu mokslininkai įrodė šio teiginio prieštaravimus, sukūrę įvairius būdus kompiuterinėms programoms problemas vertinti kaip ekspertui. Vienas iš būdų yra taisyklėmis pagrįstos sistemos, kurios sako, jog jeigu duomenys atitinka nurodytas sąlygas, reikia imtis tam tikrų veiksmų, taip pateikiant eksperto samprotavimo argumentus. Tokios sistemos modelis pavaizduotas pirmame paveiksle [41]. ES pateikia rezultatus nuosekliau nei tai daro žmogus, kadangi žmonių sprendimus lemia įvairūs faktoriai, taip atsirandant klaidų tikimybei ir poveikiui našumui [10]. Kadangi didelę dalį žmogaus mąstymo galima išreikšti taisyklėmis, toks būdas taikomas dažniausiai naudojamose šiuolaikinėse ES. Šios sistemos populiarumas išaugo ir dėl programinės įrangos gausos ir svarbiausia dėl to, jog dauguma sėkmingų sukurtų ES yra būtent taisyklėmis pagrįstos. Tai lėmė ir tai, jog trečdalis visų naudojamų ES yra skirtos diagnostikai ir tam būtent geriausiai tinka taisyklėmis pagrįstos ES [10].



1 pav. Taisyklėmis grindžiamos ES sisteminis modelis [10]

Reikėtų paminėti, jog kartais ES yra maišoma su sprendimų priėmimo sistema, o tai yra neteisinga. ES yra geros sistemos padedančios priimti sprendimus, bet tik tuo atveju, kai sprendimai yra apibrėžti sistemoje. DSS pagal savo funkcionalumą ir paskirtį yra tarp IS ir ekspertinių sistemų. Šios sistemos paskirtis yra lankstūs mechanizmai ir įrankiai informacijos gavybai ir analizei, problemų supratimui, jų galimybėms ir galimiems sprendimo būdams. DSS pateikia karkasą, kuriuo naudojantis sprendimų priėmėjai gali gauti asistavimą sprendimų priėmimui paprastu valdymu ir komandomis formuluojant alternatyvas, kuriant modelius, analizuojant atrankos poveikį. Tai leidžia sprendimų priėmėjams pasirinkti, ko jiems reikia, tiek turinio, tiek formos prasme [37].

1.1.2. ES architektūra

Kiekviena ES, nepriklausomai kur ji yra naudojama, turi dvi būtinas konstrukcines sąlygas: tos srities eksperto žinios ir įgūdžiai bei istoriniai duomenys. Taisyklėmis pagrįstos ES didžiausia dalimi, pateikiant rezultatus, pasikliauja eksperto žiniomis, o ne turimais istoriniais duomenimis. Neuroniniais tinklais pagrįstos ES didesniąja dalimi pasikliauja istoriniais duomenimis ir tik mažąja dalimi - eksperto žiniomis [41]. Papildomu ES privalumu, palyginti su paprasta programine įranga, įvardijamas žinių bazės atskyrimas nuo išvadų varikliuko (1 pav.). Kadangi išvadų varikliukas nėra kuriamas ES sistemai, kūrėjai gali susikoncentruoti ties problemos sprendimu bei turėti lengvą kartotinio sistemos tobulinimo galimybę. Tokių sistemų sėkmę įrodo pastebimas jų populiarumas verslo, inžinerijos ir medicinos srityse.

Išvadų varikliukas yra svarbi ES dalis ir gali turėti vieną ir daugiau žinių apdorojimo algoritmų ir dirbti su vienu ar keliais iš jų priklausomai nuo ES, bet žinių bazė išlieka ekspertinės sistemos šerdis. Jeigu žinių bazės turinys menkas, tokios pat skurdžios bus ir išvados [7].

Kitas ekspertinės sistemos skiriamasis ženklas yra jos galimybė pagrįsti ir paaiškinti samprotavimą. Naudojant papildomą modulį ES gali išaiškinti, kodėl vartotojas užduoda šį klausimą ir kaip sistema priėjo prie pateiktos išvados [10]. Nors ekspertinių sistemų pateikiami paaiškinimai yra visuotinai pripažinti ir buvo tarp pageidaujamų funkcijų, kuriant šiuolaikines ekspertines sistemas natūralios kalbos generavimas nėra taikomas [27].

Sprendimai ir mokymo specifika gali būti gaunami iš informacijos ir žinių, panaudojant analizės įrankius ar kitus srities ekspertus. Todėl vienas iš būdų panaudoti gautas šias žinias yra per taisyklėmis paremtas ekspertines sistemas [6].

1.1.3. ES logika

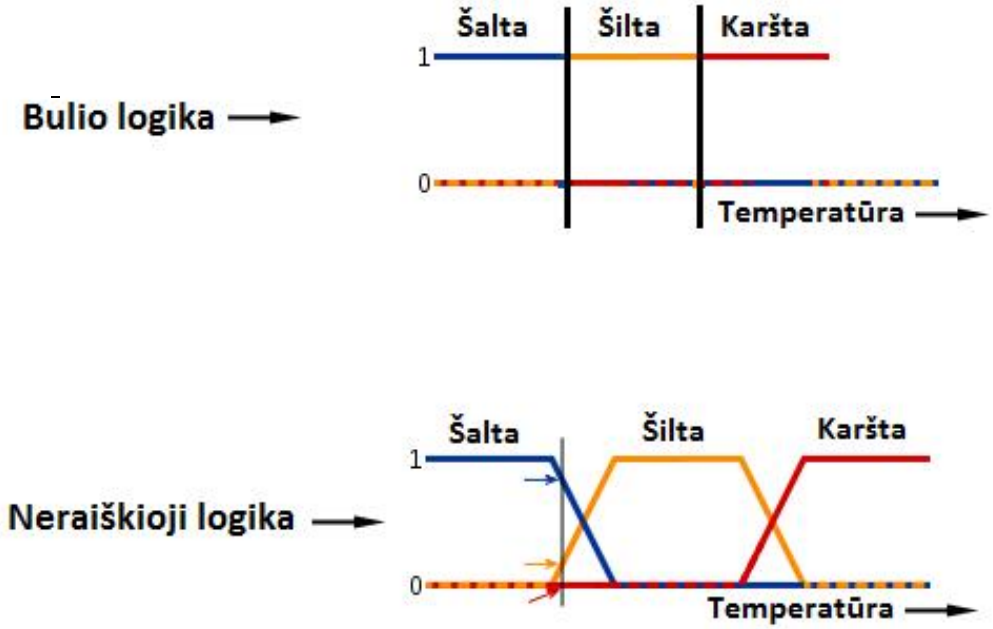
Natūrali kalba gali būti dviprasmiška ir priklausanti nuo konteksto, o žinios išreikštos taikant logikos sintaksę, yra gerai apibrėžiančios prasmę. Mokslinėse disciplinose problemos apibrėžimas, žinios apie probleminę sritį ir tikėtinų sprendinių sritį turi būti išreikštas tiksliai ir konkrečiai [29].

Ekspertinėms sistemoms evoliucionuojant įvairių tipų samprotavimo metodų buvo įtraukiama į išvadų varikliukus: Būlio logika, logika paremta ontologijomis, hipotetinis samprotavimas, neraiškioji logika. Bet dažniausiai visgi ir liko naudojama Būlio ir neraiškioji logika.

Kaip ir aukščiau minėta, ekspertinių sistemų priimamų sprendimų logika gali remtis ne vien labai paprasta Būlio logika, kurioje galimi tik tu samprotavimo variantai taip arba ne, bet ir tradicines ekspertines sistemas išplečiančia neraiškiąja logika (*angl*. fuzzy logic). Antrame paveiksle yra pateiktas pavyzdys kiek reikšmių gali turėti klausimas apie jaučiamą temperatūrą samprotaujant Būlio ar neraiškiąja logika. Neraiškiojoje logikoje atsakymas nėra vienareikšmis taip arba ne, atsakymas

pateikiamas, jeigu reikšmė patenka į tam tikrą intervalą, kuris taipogi gali būti priklausantis ne vienai reikšmei. Todėl tokią reikšmę ES turi apytiksliai suskaičiuoti ir išrinkti teisingą atsakymą iš intervalo pagal nurodytą metodą. Kaip pateikta pavyzdiniame antrame paveiksle galima pastebėti jog naudojant neraiškiąją logiką tarpuose tarp šalta, šilta arba karšta reikšmių yra galimybė gauti pereinamąsias reikšmes.

Žmonės daugumą fizinių procesų supranta remdamiesi netiksliais samprotavimais, bet tie netikslumai yra tam tikra informacija, kuri gali būti netgi labai naudinga [34]. Viskas priklauso ir nuo tikslumo poreikio, kadangi jis ne visada reikalingas, todėl galima tikslumą apsibrėžti tam tikru rėžiu ar tolerancijos riba ir taip sutaupyti sistemos, įrangos ir pan. sąskaita. Tikslumo poreikis taip pat priklauso ir nuo technologijos raidos lygio [34]. Saugos specialisto įvertinamą sistemos saugos lygį galima apibrėžti vienu tikslumu, bendro supratimo turinčio asmens apie saugos problemas kitu, o kiekybinį tikslinės sistemos saugos įvertinimą dar kitaip.



2 pav. Būlio ir neraiškiosios logikos tikslumas

Galimybė taikyti vieną ar kitą logiką priklauso nuo to, kokio tipo analizei bus naudojama sistema, kokybinei ar kiekybinei, reikalaujamo tikslumo ir ar bus keičiamos žinių bazėje esančios taisyklės ar tik bus papildoma. Taip pat pasirinkimas priklauso ir nuo galimybės versti žinias ir faktus į neraiškiąją logiką ir atgal, kadangi su neraiškiąja logika dirba ES varikliukas, o ne vartotojas. Taigi, vienas iš didžiausių neraiškiosios logikos privalumų ją naudojant ekspertinėse sistemose yra galimybė nežymiai keisti ES pateikiamus rezultatus visiškai nekeičiant taisyklių. Didėjant taisyklių kiekiui, neraiškiosios logikos pagrindu veikiančioje ekspertinėje sistemoje didėja klaidų tikimybė ir lėtėja

sistemos veikimo sparta. Taisyklių kiekis Būlio logika pagrįstose ekspertinėse sistemose įtakos klaidų atsiradimo tikimybei ar spartai nedaro.

1.1.4. Šiuolaikinės ES

Sparti interneto plėtra ir technologijų pažanga atvėrė naujų galimybių stiprinti tradicines ES. Interneto technologijos pakeitė ES kūrimo ir platinimo būdus. Dabar ES gali veikti įvairiose platformose ir būti tiesiogiai vartotojams prieinamos per žiniatinklį. Jos gali pakeisti ekspertus ten kur jų nėra dėl kokių nors priežasčių ir tai daro pakankamai efektyviai ir pigiai. Ekspertines sistemas, kaip pagalbininką, greitinantį darbą, naudoja ir patys ekspertai. Taip pat svarbus ES paplitimo faktas – žmonių ekspertų trumpalaikiškumas. Jie suserga, pakeičia darbą ar išeina iš jo. Esant įvestomis ekspertų žiniomis į sistemą, tokiu atveju galima išvengti veiklos trūkio, taip pat galima panaudoti ir esamas ekspertų žinias naujų darbuotojų mokymui [10]. Buvo prognozuota didelis ES sistemų paplitimas internete, deja, prognozės pasitvirtino tik dalinai. Didelio kiekio rimtų ES šiuo metu žiniatinklyje surasti nepavyks dėl jų sudėtingų metodologijų įgyvendinimo, kai norima, jog ES apimtų kelias sritis ir kitų sunkumų jas kuriant. Būtent tai ir mini Cernik [6] - kurti ir atnaujinti ekspertų sistemą gali būti lėtas ir skausmingas procesas. Tai reiškia, kad reikia suprasti įvairius žinių šaltinius ir ekspertinės sistemos kalbos sintaksę bei semantiką. Jau vien šis faktas parodo, kad yra pakankamai sunku sukurti ekspertinę sistemą ir dar sudėtingiau išmokyti kompiuterį savarankiškai tokią sukurti. Būtent šių priežasčių pakanka, kad potencialūs kūrėjai nusigręžtų nuo ES, vien dėl laiko sąnaudų pačiai sistemai sukurti [6]. Tačiau reikėtų pastebėti, jog dabar jau pasirodo įrankių internetinių ES kūrimui, nereikalaujančių visai jokių ES kūrimo žinių [35].

ES naudojamos žinios dažnai yra kilusios iš tam tikros srities ekspertų. Ankstyvosios žiniomis paremtos sistemos iš tikrųjų ir buvo kurtos glaudžiai bendradarbiaujant su ekspertais, tai nulėmė ir pirmųjų dienų ES terminą, kuris vartojamas šioms sistemoms apibrėžti. Žinios taip pat gali būti gaunamos iš literatūros, ar iš duomenų rinkinių, surinktų mašinomis. Be to, ne visos konkrečių ekspertinių sistemų sritys gali būti žiūrimos kaip specialistų sritys. Dėl šios priežasties kai kurie autoriai įvardija ir atskiria ekspertines sistemas nuo žiniomis grindžiamų sistemų. Jų nuomone, pastaroji yra daug bendresnio pobūdžio nei ekspertinė sistema, kuri visada apima specialisto srities lauką [26; 36; 15].

Tačiau ekspertinės sistemos nėra be trūkumų. Iš išlikusių trūkumų nuo ES sistemų atsiradimo galima paminėti ne visada aiškias ir nematomas sąsajas tarp taisyklių. Nors atskiros taisyklės linkusios būti gana paprastos ir aiškios, jų loginė sąveika, esant dideliam taisyklių rinkiniui, gali būti neskaidri. Taisyklėmis pagrįstose sistemose sunku stebėti, kaip atskiros taisyklės lemia bendrą strategiją. Taisyklėmis pagrįstose ekspertinėse sistemose tai lemia hierarchinių žinių atvaizdavimo trūkumas. Dar vienas taisyklėmis pagrįstos ekspertinės sistemos trūkumas - nesugebėjimas mokytis iš patirties.

Skirtingai nuo žmogaus eksperto, kuris žino, kada laužyti taisykles, ekspertinė sistema negali automatiškai modifikuoti, pritaikyti esamas taisykles ar pridėti naujų žinių į bazę. Žinių inžinierius vis tiek reikalingas prižiūrėti ir palaikyti sistemai [28].

1.2. ES taikymas saugos valdymui

Per pastaruosius dvidešimt metų buvo nemažai mėginimų siekiant sukurti ar pagerinti ekspertines sistemas, skirtas informacijos saugai užtikrinti, valdyti ir rizikai įvertinti. Deja, iki šiol nėra jokios rimtos šios srities ekspertinės sistemos, kuri pašalintų ekspertą ar net leistų išvengti žmogaus intervencijos. Svarbu pridurti, jog iki šiol nėra rimtų ES, skirtų saugos valdymui bendrąja prasme.

Kai kuriuose naujausiuose leidiniuose minima, kad ekspertinės sistemos ir AI panaudojimo būdai dar tik pradėti tirti ir turi daug ką pasiūlyti informacijos saugos problemų specialistams.

Didžioji dalis literatūroje randamų ES yra taikytinos IT saugos valdymui ir skirtos tam tikrai verslo sričiai ir integruotos į verslo valdymo sistemas. Likusioji dalis literatūroje aptariamų ES yra skirtos bendriems informacijos saugos klausimams spręsti ir yra eksperimentinio, mokslinio, modelinio ar koncepcinio pobūdžio.

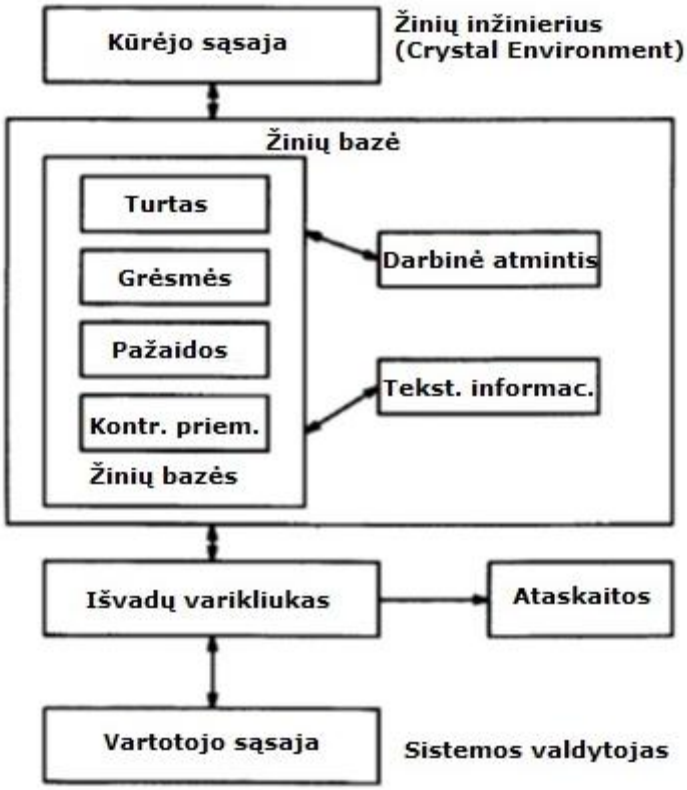
ESISA - viena iš paprastesnių ir bendresnių ES, skirtų saugos valdymui. Ji paremta ISO 27K standarto klausimynu, išskirstytu pagal kontrolės tikslus. Kaip mini autoriai, ES skirta plataus masto auditui, yra sudėtingesnė nei klasikinė ES, kadangi joje reikia aprašyti kompleksiškesnes saugos įvertinimo procedūras, kurios apima daugelį veiksnių. Autoriai pasirinko neraiškiąja logika pagrįsta ES, kadangi informacijos saugos ekspertai paprastai manipuliuoja apytikslėmis sąvokomis. Sistemoje taisyklių skaičius yra lygus priežasčių kiekiui tiek, kiek pažaidų gali lemti nurodytą grėsmę. Sistemos klausimuose ir išvadose yra naudojami netikslūs raktiniai žodžiai, kurie gali giliai ir aiškiai rodyti pateikto klausimo ar rekomendacijos prioritetą [21].

SISMS - išmani informacijos saugos valdymo sistema. Ji yra **ENISA** rekomenduojamų rizikos valdymo, rizikos vertinimo priemonių sąraše. SISMS yra visą informacijos saugos valdymą apimantis programinės įrangos paketas, kuris naudoja ekspertinę sistemą nustatant, įgyvendinant, eksploatuojant, stebint, peržiūrint, prižiūrint ir pagerinant informacijos saugos valdymą. Ji paremta tarptautiniu standartu ISO 27001 [19]. Sistema tikrina organizacijos tinklą, įskaitant visą techninę įrangą, informaciją (operacinės sistemas, specifikacijas, veiklą ir jos efektyvumą, našumą), nuskaito atvirus arba filtruojamus TCP ir UDP prievadus ir paslaugas, pateikia atvirų prievadų paslaugų versijas. Be to, ji pagal gautą tinklo nuskaitymo informaciją, pateikia organizacijos tinklo žemėlapį. Iš esmės sistema turi tris pagrindines funkcijas: tinklo stebėseną, tekstinio tipo papildomus modulius, kuriais nustatomi kiti reikalavimai ir veiksmai, kurių turi būti imtasi pagal ISO 27002 (2005) standartą ir išmanių programų, nustatančių organizacijos saugos būklę. Visa informacija talpinama duomenų

bazėje, kuria naudojasi CLIPS pagrindu veikianti ES, siekiant nustatyti esamą organizacijos saugos būklę. Organizacijos kontrolės reikalavimai ir taisyklės, kuriomis siekiama įvykdyti šiuos reikalavimus, remiasi ISO 27001 ir ISO 27002 atitinkamai [19].

Pagrindiniai programinio paketo minusai yra: sistemą turi naudoti geras IT žinias turintis darbuotojas; sistema privalomai adaptuojama prie kliento ir sistemos tobulinimas galimas tik paties gamintojo pagal galutinio vartotojo pasiūlymus. Paskutinis minėtas punktas prieštarauja sistemos aprašyme pateiktai informacijai, jog ji plačiai apima bendrus informacijos saugos valdymo procesus.

Ramex – tai ekspertinės sistemos prototipas, skirtas kompiuterių saugos rizikos analizei ir valdymui mažoms ir vidutinėms komercinėms organizacijoms. Šio įrankio kūrimą paskatino tokių sistemų trūkumas. Ramex prototipas buvo kurtas remiantis anksčiau atliktais tyrimais ir kaip pagrindą laikant straipsnį - kokybinės rizikos analizės taikymas kompiuteriniam saugumui komerciniame sektoriuje [3]. Ramex sistemos tikslas - atlikti kokybišką saugos vertinimą, susijusį su tarptautinėmis grėsmėmis, ir pateikti ataskaitas kokių atsakomųjų priemonių turi imtis valdymo organai. Ramex turi greitai atlikti neformalius tyrimus, būti ekonomiškai efektyvus ir praktiškas valdymo įrankis [20]. Tam, kad būtų išvengta sudėtingumo, įrankio terminijai pasinaudota ITSEC ir DTI pateikiamais terminais, nors tuo metu, kai sistema buvo kuriama, terminija buvo jau pakankamai standartizuota. Įrankis buvo kuriamas kaip atskirai įdiegiama sistema. Grėsmės klasifikuojamos į tris grupes: gamtos nelaimes, netyčinės žmonių klaidos ir tyčinė žmonių veika. Didžiausias dėmesys sutelkiamas į paskutiniąją grupę. Sistemos rizikos analizė ir valdymo metodologija sukurta iš septynių žingsnių: turto identifikacija, grėsmių identifikacija, pažaidų identifikacija, identifikacija esamų saugos priemonių, poveikio verslui įvertinimas, taikytinų saugos priemonių įvertinimas ir ataskaitos generavimas. Trečiame paveiksle pavaizduota RAMeX žinių bazės struktūra, kurią sudaro vertybių, grėsmių, pažaidų ir atsakomųjų priemonių žinių bazės. Darbe minima, jog tokia žinių bazės struktūra palengvina kintamųjų apsikeitimą tarp pačių duomenų bazių ir darbinės atminties.



3 pav. RAMeX struktūra [20]

Ekspertinė sistema kurta Crystal taisyklėmis pagrįstos ekspertinės sistemos pagrindu. Komunikacija su vartotoju atliekama klausimų ir pateiktų atsakymų pažymėjimo būdu. Sistemos taisyklės sukurtos vertybes išskirsčius į šešias kategorijas. Įvedus reikiamą informaciją yra sukuriamos matricos. Vartotojas gali analizuoti sukurtas kelių lygių matricas, taip pasirinkdamas detalumo lygį, pagal kurį matomos grėsmės visai turto grupei ar pogrupiui. Pasinaudodama matricomis sistema klausia vartotojo, kurios sugeneruotos grėsmės ir turto poros yra potenciali rizika. Gavus visus atsakymus sistema toliau analizuoja duomenis ir pateikia rezultatų ataskaitą.

Nors įrankio kūrėjai moksliniame straipsnyje ir teigia esantys pažengusiame įrankio kūrimo etape bei planuojantys sistemos veiksmingumą padidinti integruojant daugiau rizikos analizės aplinkų, taip išplečiant sistemos panaudojimo ribas, daugiau apie sistemą informacijos taip ir nepateikta. Straipsnis labai dažnai cituojamas kituose darbuose apie ES.

Audes – eksperimentinė ekspertinė sistema skirta saugos auditui. Sistema pagal savo paskirtį yra viena iš procedūrų, skirtų saugos valdymui. Straipsnyje aprašomas Audes ekspertinės sistemos projektas sukurtas išanalizavus kompiuterių saugos audito srityje esamas ekspertines sistemas. Audes yra skirta automatizuoti rankinio saugos audito procedūroms ir sumažinti žmonių įnašą bei klaidas, kurios atsiranda žmonėms operuojant dideliu žinių kiekiu. Ji ne vien identifikuoja problemas, bet ir iškelia identifikuotas problemas į viršų ir atlieka nurodytus veiksmus joms šalinti. Sistema taip pat gali panaudodama išorines funkcijas iš ES atlikti nurodytas įspėjimo funkcijas. Galutiniame audito etape

auditorius patvirtina atliktą audito procedūrą ir sistema viską suarchyvuoja. Audes yra tarpininkas tarp auditoriaus ir rankinio sistemų saugos įrankio RACF. Ši sistema orientuota į sistemai nurodytų veiksnių aptikimą ir tęstinų veiksmų siūlymą [42].

Ekspertinė sistema sukurta naudojantis komercine ESE aplinka, kuri pasirinkta dėl sėkmingo sistemos pritaikymo diagnostikai, planavimui ir sprendimų priėmimui ir ne mažiau svarbios sistemos galimybės, suteikiančias plačias sąsajas su išorinėmis procedūromis. Svarbi sistemos dalis - paaiškinimo modulis, kuris vartotojui leidžia užduoti klausimus apie sistemos atliktus veiksmus. Visi paaiškinimai ir kelias iki išvadų sistemoje automatiškai registruojami ir įrašomi vėlesniam peržiūrėjimui ir naudojimui taip supaprastinant kasdienes užduotis.

Visos sistemos naudojamos žinios ar taisyklės yra paimamos iš RACF. Kadangi kompanijos kurios naudoja RACF, yra didelės, tokiose kompanijose visos saugos audito procedūros yra dokumentuotos, stengiantis apimti visus galimus scenarijus. Kaip mini autoriai, sistema turi galimybę audituoti daugiasistemiškai, taip išvengiant būti nepastebėtiems bandymams pažeisti kiekvieną sistemą distribiutyviai iki tam tikro lygio, kol tai neperžengia sistemų reagavimo slenksčio.

Didžiausias šios sistemos trūkumas yra jos susiejimas prie RACF ir žinių bazės atnaujinimas, kuris galimas tik per šią sistemą. Nors straipsnyje kalbama apie sistemos panaudojimą keliose sistemose, neužsimenama, jog visos jos turi būti RACF. Kita vertus, sistema buvo kuriama IBM mokslo centre, orientuojantis į įmonės produktus. Išskirtinai šios sistemos naudotojams tai yra sistemos privalumas, kadangi visa žinių bazė yra imama iš paplitusios auditavimo sistemos, taip turint galimybę gauti naujausias žinias ir jas nesudėtingai perkelti į ES [42].

IDES, NIDES – tai specifinės, dažnai moksliniuose darbuose minimos ES, skirtos įsilaužimui aptikti. Minimos sistemos yra daugiau identifikacinio pobūdžio. Jos nepateikia pasiūlymų identifikuotoms problemoms spręsti, neidentifikuoja rizikų, o tik pateikia patį įvykį. Todėl prasmės jas analizuoti giliau nėra [25].

Wynyard Risk 9 – tai rizikos valdymo platforma, kurioje esti iš karto įdiegti informacijos saugos valdymo ir išplėtotos politikos valdymo moduliai. Platformoje iš karto sukonfigūruota rizikos valdymo sistema, paremta ISO 27001 standartu, taip pat ir kiti papildomi moduliai, rekomenduotini vyriausybės kibernetinės saugos įstaigų. Tai nėra ekspertinė sistema, o tiksliau informacijos saugos valdymo priemonė, kurioje yra pritaikytos tam tikros ekspertinės sistemos dalys. Naudojant platformą galima sisteminti rizikos identifikavimo, tikimybės ir masto poveikio procesus, taip supaprastinant reagavimą į svarbius procesus, stebėti konkretaus proceso pažangą ir patį rizikos mažinimo procesą. Sistemoje yra fiksuojami visi buvę ir esami incidentai, dingę dokumentai ir pan., kurie nulemia sistemos pateikiamus rezultatus ir išvadas. Taip pat naudojantis platformos analitiniu moduliu, galimi įvairūs ataskaitų pjūviai.

Mažų įmonių ES pateiktą vertinimą galima vertinti ir kaip bendrą įmonės riziką. Pavyzdžiui, elektroninės parduotuvės, kuri yra tarpininkas tarp galutinių klientų ir tiekėjų. Tai galima pamatyti, nagrinėjant EC šaltinį [32]. Šiame dokumente aprašoma neraiškiąja logika pagrįsta sprendimų priėmimo sistema, kuri galėtų būti naudojama projektų vadovų efektyviai ir veiksmingai atlikti rizikos vertinimą, plečiant elektroninę komerciją. Minimo darbo motyvacija atsirado dėl tokios sistemos trūkumo ir dėl to, jog EC yra iš esmės nauja sritis, todėl dauguma įmonių turi tik ribotą informaciją, susijusią su rizikos įvertinimų. Esami rankiniai metodai reikalauja didelių laiko sąnaudų, o kartais ir papildomo darbuotojo. Tuo skundžiasi dažnas projektų vadovas ir visada nerimauja dėl rezultato, kadangi dėl rizikos analizės sudėtingumo negalima jos vykdyti bet kuriame projekto raidos etape. Todėl buvo nutarta sukurti sistemą, kuri padeda įvertinti įmonės rizikos lygį automatiškai ir suteikia galimybę visą EC kūrimo laikotarpį bet kuriuo projekto etapu lanksčiai atlikti bendrą rizikos įvertinimą. Rizikos analizė gali būti atliekama, naudojant tikimybių teoriją [32].

Apžvelgtoje literatūroje pastebėta, jog ES sistemas vis dažniau bandoma integruoti į valdymo sistemas ir leisti joms pateikti pasiūlymus, įspėti apie problemą sistemą prižiūrinčius asmenims. Informacijos saugos valdymą didesnės įmonės išskirsto į kelias dalis:

1) *Informacijos saugos sertifikacijos;*

2) *Nuolat atnaujinami programinės įrangos paketai skirti tinklo, programinės įrangos, specifinių pažaidų aptikimui;*

3) *Ir galiausiai tik didžiausios rizikos srities ES pritaikytos konkrečios įmonės tipui*.

Mažos ir vidutinės įmonės sau to leisti negali. Kita minėtų sistemų trūkumo pusė, susijusi su verslo dydžiu, yra ta, jog mažose įmonėse visų procesų aprašyti nėra galimybės. Tas pats ir su informacijos saugos scenarijais, siekiant viską išsiaiškinti ir aprašyti prieš imantis veiksmų. Nors dabar jau teigiama, kad sistemoms kompleksiškėjant net ir didelės kompanijos nebepajėgia aprašyti ir išanalizuoti visų scenarijų, todėl pradeda naudoti bendras saugos specialistų kuriamas žinių bazes. Kaip ir anksčiau minėta, tokios sistemos naudojamos kaip pagalbininkas arba pasitikslinimo ir pasitikrinimo galimybė.

Didelė dalis mokslinio lygmens sistemų nors ir deklaruojamos, kad jos yra ekspertinės sistemos, skirtos taikyti verslo informacijos bendriems saugos valdymo procesams, vis tiek yra specializuotos ar skiriančios didesnį dėmesį tam tikrai sričiai. Dalis sistemų riziką įvertina remdamasi ES naudotojo pateiktais duomenimis, kita dalis rizikos laipsnį leidžia įvesti pačiam sistemos naudotojui. Verta paminėti dar vieną ES sistemų grupę, skirtą ankstyviems IS planavimo ar įgyvendinimo etapams, koncentruojantis į pasirenkamą architektūrą, saugos priemones, pasirenkamą saugos lygį.

Galima teigti, jog šiuo metu ES, pritaikytos informacijos saugos valdymui mažose ar vidutinėse įmonėse, apimančiam visą įmonės informacijos saugos politiką, nėra, o ypač bendros paskirties, galinčių prisitaikyti prie naudojamos aplinkos ir verslo sąlygų pasikeitimo.

Palyginti ir išanalizuoti aptartų sistemų privalumus ir trūkumus yra sunku, kadangi visos sistemos savo tikslu yra skirtingos. Analizuojant bendrai, t.y. neišskiriant sistemų skirtumų, galima teigti, jog panaudojus Ramex modelį, ESISA saugos standartų integraciją į sistemą ir SISMS, panaudotą žinių bazės valdymo modelį, tokia sistema būtų pranašesnė už visas aptartąsias.

1.3. ES taikymas gretutinėse srityse

MYCIN – verta trumpo aptarimo kaip labiausiai internete aptariama ekspertinė sistema pionierė. MYCIN yra tradicinė labai siauros srities ES, skirta infekcijų gydymui, padedanti nuspręsti, kokio didumo infekciją turi pacientas, nustatyti galimus organizmo pažeidimus, pasirinkti labiausiai tinkamus vaistus ir jų kiekį. MYCIN žinių bazė buvo sudaryta iš keturių šimtų penkiasdešimties taisyklių. MYCIN prilygo ekspertui ir buvo žymiai geresnė identifikuojant infekcijas nei jaunesnieji daktarai, bet realiai sistema panaudota pagal paskirtį taip ir nebuvo, nors jos tikslumas siekė apie septyniasdešimt procentų [10; 28]. Tokios ES pavyzdys, gali būti kaip šaltinis taikant kenksmingo programinio kodo ar panašių saugos problemų analizavimui ir taikomų saugos priemonių parinkimui įmonėje.

IES - ne techninių nuostolių integruota ES, vienas iš integruotų ES pavyzdžių. Sistema yra naudojama elektros tiekimo įmonėje analizuoti sukauptą informaciją nesąžiningų vartotojų išaiškinimui. ES sprendimams reikalinga informacija yra gaunama iš įvairių analizės programų, kurios informaciją ima iš įmonėje esančių dokumentų, matavimo įrangos, inspektorių išvadų. Taikant tokią ES sistemą, sugebama aptikti du kartus daugiau nesąžiningų vartotojų nei analizę atliktų ekspertai, kadangi šios užduoties sudėtingumas remiasi milžiniško informacijos kiekio apdorojimu. Dėl milžiniško informacijos kiekio ekspertai koncentruojasi į bendrą visumą, o ne į detales. Todėl ES sistema tokiu atveju padeda rasti smulkiausias detales, leidžiančias daryti tikslesnes išvadas [24]. Aptariamos ekspertinės sistemos aktualumas šiame darbe aptariamai problemai yra tas, jog naudojant istorinius duomenis ir tam tikrus faktus, ieškant atsakymų, galima koncentruotis ne vien į visumos analizavimą bet ir atkreipti dėmesį į atskiras detales.

Hidraulinių sistemų diagnostikos ES – skirta nesklandumų detekcijai, prognozei, kompensacijai ir diagnostikai. Sistema ne tik pateikia išvadas, bet ir automatiškai realiu laiku stebi ir kontroliuoja hidraulinę sistemą [2]. Aptariama sistema parodo, jog taikant ekspertinę sistemą galima ne tik diagnozuoti iš pateikiamų rezultatų, o ir pagal pateiktus rezultatus tiesiogiai valdyti sistemas.

Problemų sprendimo naudojantis interneto paieška ES – sistema, skirta padėti studentams, efektyviau ir taupant laiką spręsti iškilusias problemas, naudojantis paieškos internete galimybėmis. Sistema sukurta išsiaiškinus, jog didelė dalis studentų paiešką atlieka neefektyviai, stokojant tikslumo, taip gaištant laiką paieškai, o ne studijoms. Sistema veikia kaip instruktorius, pateikdama pasiūlymus, padėsiančius pagerinti studentų paieškos rezultatus. Sistemos žinių bazė sukurta automatizuotai surinkus studentų atliktas užklausas, ekspertams jas išanalizavus ir pavertus į taisykles, kurios sudėtos į ES [16]. Sistema yra geras pavyzdys, jog ES galima panaudoti ne tik, kaip pavyzdys saugos valdymui, bet ir darbuotojų informacijos saugos instruktažui.

ES motyvuojanti neapibrėžtumais – sistema skirta augalų ligos diagnozavimui. Pažymėtinas sistemos bruožas, kad ji atsižvelgia tiek į duomenų, tiek į procesinių žinių neaiškumą, kas padeda diagnozuoti ligas ankstyvojoje stadijoje. Tam pasiekti sistema naudoja įvairių laipsnių apibrėžtumo ir tikslumo faktų ir taisyklių pateikimo metodologijas ir formalizmus. Sistema gali būti naudojama tiek vartotojo hipotezei įvertinti, tiek mokymosi tikslais [43]. Aptariamos sistemos atžvilgiu pakankamai svarbi savybė, kuri gali būti panaudota ir saugos valdymo ES, yra įvairių laipsnių neapibrėžtumo panaudojimas.

Teisės ES - internete veikianti konsultacinio tipo, teisinių problemų sprendimo ES. Ji yra viena iš sėkmingesnių ekspertinių sistemų, veikiančių internete pavyzdžių, gaunanti dideles pajamas. Teigiama, jog sistema kainuoja tiek pat, kiek kainuoja pradedantysis teisininkas pirmaisiais darbo metais [5]. Iš šios ekspertinės sistemos galima suprasti, jog gerai susisteminus žinias ir jas teisingai pritaikius ekspertinėje sistemoje, net ne tos srities specialistas, pateikdamas faktus neprofesine kalba, gali greitai gauti tikslius eksperto lygio atsakymus.

RATS – ekspertinė sistema skirta naujų telekomunikacinių paslaugų kūrimo asistavimui. Ji padeda pirmomis paslaugų kūrimo fazėmis kai yra renkami ir analizuojami paslaugos reikalavimai. Sistema taip ir liko prototipu [11]. Sistemos prototipas parodo, jog ekspertinė sistema taip pat gali būti naudojama asistavimui, o ne konkrečių rezultatų pateikimui.

PORSEL – ES skirta investicijų analizavimui ir įvertinimui. Sistemą sudaro trys komponentai: informacijos centras, neraiškiosios logikos akcijų selektorius ir portfelio konstruktorius. Informacijos centro komponentas pateikia techninius rodiklius, tokius kaip kainų tendencijos, slenkamasis vidurkis. Neraiškiosios logikos selektorius įvertina išrinktas akcijas ir prie kiekvienos iš jų prideda sudėtinę reikšmę. Portfelio konstruktorius pagal gautas reikšmes sukuria optimalų akcijų portfelį iš pasirinktų akcijų. Sistemos taisyklės sukurtos paieškai pagal tam tikras neraiškiosios logikos reikšmes, labiausiai atkreipiamas dėmesys į per mažai įvertintas akcijas, kurių potencialas neįžiūrėtas. Atliktas eksperimentas su sistema, panaudojus trylikos metų istorinius akcijų biržos duomenis, parodė, jog sistema savo įžvalgumu aplenkė Standard & Poor's 500 akcijų rinkos indeksą. Kaip tokiai paprastai ES tai didelis pasiekimas [44]. Ši sistema akivaizdžiai parodo, jog ekspertų žinias pavertus taisyklėmis

ir kartu su DSS tipo istorinėmis žiniomis jas patalpinus į ekspertinę sistemą, gaunami puikūs rezultatai, kas gali būti pritaikyta saugos valdymo ES.

Tarantula – ES skirta kenksmingo programinio kodo aptikimui. Kaip mini autoriai, tokią sistemą pristatyti paskatino sudėtingėjantis ir didėjantis kenksmingo programinio kodo bandinių skaičius, kas sudaro sunkumų naudoti parašų bazę tokio kodo aptikimui. Tam išvengti, nuspręsta taikyti elgsenos stebėjimu pagrįstą ekspertinės sistemos modelį. Ekspertinė sistema veikia stebėsenos ir veiklos užtikrinimo sluoksnyje. Programos taisyklės paremtos dažniausiais ir populiariausiais kenksmingo programinio kodo bandymų tipais pasinaudoti kritiniais sistemos ištekliais, tokiais kaip failų sistema ar operacinės sistemos registrai. Kadangi sistema stebi visus sisteminius iškvietimus, ji pastoviai naudoja sistemos resursus, kurie pagal atlikus tyrimus papildomai gali sudaryti iki dvidešimties procentų. Tokia sistema yra labai geras ES integravimo į universalias sistemas pavyzdys [33].

FRBCES – tai neraiškiąja logika paremta ES, skirta identifikacijai problemų, kibernetinio saugumo klausimais. Potencialių ekspertinėje sistemoje aprašomų grėsmių sąrašą sudaro: kenksmingo programinio kodo, DoS, trojos arklio, konfidencialių duomenų perėmimo, paslaugos nepasiekiamumo, sistemos kontrolės perėmimo ir socialinės inžinerijos. Iš viso minėto grėsmių sąrašo darbe visgi pagrindinis dėmesys skiriamas įsilaužimų, DoS ir sistemos nepasiekiamumo grėsmėms. Neraiškiajai logikai išreikšti naudojamas MATLAB neraiškiosios logikos įrankis. Įrankis naudojamas ne tik ES kūrimo metu, bet ir vartotojų faktų įvedimui ir rezultatų pateikimui, todėl sistema tikrai skirta tik pažengusiems, kaip minima darbe - sistemų administratoriams ar kitiems specialistams dirbantiems su MATLAB. Sistema pateikdama rezultatus iš neraiškiosios logikos į lingvistinius kintamuosius išreiškiami surandant paprastą minimalios ir maksimalios neraiškiosios logikos reikšmės vidurkį. Tai parodo abejotiną tokios logikos panaudojimo tikslingumą [14].

Sistema kibernetinių grėsmių paieškai ar elementariam kylančių grėsmių ir naudojamų saugos priemonių prieš jas identifikacijai yra tikrai tinkama. Kalbant apie sistemos tinkamumą kibernetinei saugai užtikrinti, nenaudojant jokių išorinių duomenų, kuriais būtų galima remtis nustatant aktualias grėsmes, yra labai abejotina [14].

ES modelis, skirtas **komercinio debesų paslaugos tiekėjo pasirinkimui** – viena iš sudėtingesnių ekspertinių sistemų, kuri padeda apsispręsti, taikant išlaidų ir gaunamos ekonominės naudos principą, renkantis debesų paslaugos tiekėją. Toks darbas darosi vis labiau svarbus ir ne mažiau sudėtingas nei renkantis paprastas kompiuterines sistemas. Sistemos sudėtingumas kyla iš jos architektūros ir ciklinio nurodytų atvejų (*angl*. case) samprotavimo proceso.

Sistemoje žinios talpinamos duomenų bazėje ir žinių bazėje. Duomenų bazėje talpinami išspręsti, sprendžiami ir iš anksto ES kūrimo metu pilnai aprašyti debesų paslaugos tiekėjo pasirinkimo atvejai. Aprašyti atvejai yra su ir be atliktais įvairiais tyrimais, bei surinktos pavyzdinės tiekėjų

pasirinkimų praktikos. Žinių bazėje yra talpinamos taisyklės, konkrečiai apimančios kažkurį parametrą, kriterijų ir panašiai. ES samprotavimas taikant žinių bazę, yra analogiškas ankščiau aprašytoms sistemoms. ES samprotavimas, taikant duomenų bazėje esančius atvejus, yra sudarytas ir apimantis keturis etapus: duomenų bazėje esančių atvejų ištraukimas, ištrauktų atvejų panaudojimas, atvejo sprendimo patikrinimas su nauju analizuojamu atveju (esant atitikimams analizuojamo atvejo papildymu), papildomos informacijos įtraukimui į duomenų bazę. Atvejų iš duomenų bazės ištraukimui ir pritaikymui naudojami trys išrinkimo metodai: tikslusis, euristinis ir neraiškiosios logikos. Metodai pritaikomi eilės tvarka, kol gaunamas reikalingas rezultatas, o jo negavus duomenų bazės atvejai rezultatų nelemia. Taikant euristinį ir neraiškiosios logikos modelį, tikslinimui naudojamos žinios iš žinių bazės. Toks ES veikimas yra labai tikslus, net ir tuo atveju, jeigu žinomų atvejų yra nedaug [30]. Šios sistemos taikomas atvejų pritaikomumas analizuojamoje situacijoje, yra svarstytinas saugumo valdymui skirtoje ES. Kaip pavyzdys tai galėtų būti kaip konfliktines situacijas tikslinančios taisyklės iš ekspertų.

IT projektų rizikos įvertinimui skirta **ES** – neraiškiąja logika pagrįsta ekspertinė sistema, skirta padėti nustatyti informacinių technologijų projektų rizikos lygį pagal pateiktus kintamuosius. Anot autorių, sistemos kūrimui pasirinkta neraiškioji logika dėl ekspertų pateikiamų sprendimų ne konkrečiais kintamaisiais, o kalbiniais kintamaisiais. Ekspertų išvados žinių bazės pildymui yra apdorojamos FIS neraiškiosios logikos MATLAB aplinkos įrankiu, taip gaunant į neraiškiąja logika išverstas ekspertų žinias. Rizikos lygiui nustatyti sistemoje kategorizuojami šeši pagrindiniai rizikos faktoriai, kiekvienas iš jų atskirai turintis dar po dvidešimt aštuonis projekto rizikos subfaktorius. Empirinis sistemos tyrimas atliktas Irano Saman banke [31].

DIABRA – ekspertinė sistema skirta padėti nustatyti II tipo cukrinio diabeto susirgimo riziką. Sistema taiko kiekybinį modelį, kuris analizę atlieka pagal parengtus scenarijus. ES sukurta per keturis etapus: rizikos faktorių identifikacija, žinių įgijimas taikant analitinį hierarchinį procesą (AHP), surinktų žinių vaizdavimo ir sistemos validacijos. Taip pat autoriai mini, jog ES yra geras įrankis, kuris gali būti naudojamas kaip prevencinė priemonė, pateikianti patarimus kaip sumažinti tikimybę susirgti cukriniu diabetu. Turint tokio tipo ir tokio baigtinio lygmens žinias, ekspertinė sistema yra lygiavertė realiam ekspertui [1]. Kaip ir MYCIN atveju, tokia sistema parodo ES galimybes būti ne vien identifikavimo, bet ir prevencine ar patariamąja priemone. Svarbu, norint gerų rezultatų, naudoti tam tikrą žinių susisteminimo metodą.

Sunku surasti sričių, kuriose ES nėra taikoma. Apibendrinant, pagal visus naujus trejų metų mokslinius straipsnius, galima teigti, kad didžioji diduma tyrimų ES atžvilgiu yra medicinos srities. Toks ES taikymo populiarumas medicinos srityje dėl savo kompleksinių problemų taip pat padeda atsirasti ir papildomų ES funkcijų, tokių kaip sprendimų priėmimas pagal keletą kriterijų (MCDM), kas leidžia išplėsti tokios sistemos panaudojimo sritį.

Šiek tiek mažau ES tyrimų yra elektronikos ir IT diagnostikos srities, tačiau vis didėjanti ES tyrimų dalis, skirta įvairių mechanizmų diagnostikai. Taip pat ES susidomėjimas jaučiamas ir įvairių sričių rizikos vertinimui. Tai bankai, investicijų įmonės, darbuotojų paieška, akcijų birža [9]. Ekspertinės sistemos panaudojamos vis įvairesnėse srityse. Didieji mokslinių leidinių leidėjai leidžia specialius žurnalus, skirtus ekspertinėms sistemoms ir tyrimams žinių ir jų bazių rinkimui apžvelgti. Taip pat jaučiamas ES integracijos padidėjimas į bendras sistemas ir jų žinių kaupimas naudojant vidinę sistemų informaciją, aprobuotą ekspertų. Visos išvados yra darytos remiantis Wiley, Springer, Elsvier pateikiamų mokslinių straipsnių ir knygų duomenimis.

1.4. ES pritaikomumas rizikos valdymui

Pagal ISO 27005 [18], informacijos saugos rizika yra apibrėžiama kaip potencialas, kad tam tikra grėsmė išnaudos turto ar turto grupės pažaidą ir tokiu būdu pakenks organizacijai. Rizikos valdymo proceso tikslas yra nustatyti šias rizikas, įvertinti jų atsiradimo tikimybę, o tada imtis veiksmų, kad pavojus būtų sumažintas iki priimtino lygio. Visi rizikos analizės procesai naudoja tą pačią metodiką. Iš pradžių yra nustatomas ir peržiūrimas visas turtas. Nustatomos rizikos, problemos, grėsmės, pažaidai. Įvertinama rizikos atsiradimo tikimybė ir galimas jos poveikis tam turtui ar organizacijai, jeigu ji būtų įgyvendinta. Tada nustatoma kontrolė, kuri turi priartinti galimą poveikį iki verslui priimtino lygio [4].

Sutrumpintai galima teigti, jog rizikos valdymas apima tris procesus: rizikos vertinimo, rizikos mažinimo, analizės ir atestavimo. Informacijos saugos rizikos vertinimas yra būtinas procesas saugos valdyme, kadangi finansiniai ištekliai yra riboti ir juos reikia skirti, svarbiausių vertybių, grėsmių ir pažaidų mažinimui. Vertinimas leidžia sudėti visus rizikos vertinimo aspektus į vieną visumą. Žinant priimtiną verslui rizikos lygį tam tikrai vertybei, galima nustatyti pritaikomas ar diegtinas priemones ir jų prioritetus. Darbe minima ES realiai atliks tik pirmąjį iš išvardintų procesų, bei pateiks pasiūlymus rizikos mažinimo procesui, todėl toliau svarbu giliau panagrinėti rizikos vertinimo procesą.

Pagal ISO 27005, rizikos vertinimas - tai bendras rizikos identifikacijos, rizikos analizės ir rizikos įvertinimo procesas. Darbe aprašoma ES turi būti pilnavertis įrankis informacijos saugos valdymui su sąlyga, kad sistema atliks pilną rizikos vertinimą ir tik dalį rizikos valdymo, pateikiant pasiūlymus ir veiksmus ES vartotojui. Tai reiškia, jog sistema turi ne tik identifikuoti grėsmes, galimas pažaidas, bet ir įvertinti riziką jiems įsigyvendinti pagal sistemos turimas žinias. Po šio proceso ES sistemos vartotojas gali priimti pateiktą liekamąją riziką arba spręsti, ar konkretaus proceso ar sistemos naudojimas yra priimtinas atsižvelgiant į pateikiamą riziką. Todėl sistema neturėtų apsiriboti vien rizikos tipų pateikimu, bet ir nurodyti rizikų skirtumus taip, kad būtų suprantama ir ne specialistui.

Rizikos vertinimas, šio darbo atveju, yra dialogas tarp ES naudotojo ir ES sistemos, sistemai pateikiant pagrįstas išvadas su paaiškinimais. Vartotojo rizikos vertinimas yra tiesiogiai susijęs su ES turimomis žiniomis ir esant dideliam rizikos vertinimo neatitikimui tarp vartotojo duomenų ir ES sistemos, yra atmetama subjektyvi vartotojo nuomonė.

Tariant supaprastintai, rizikos analizę, kuri yra taikoma ir dabar naudojamose ES rizikai valdyti, galima išskaidyti į keturis uždavinius:

1. *Identifikuoti vertybes;*
2. *Identifikuoti rizikas;*
3. *Prioritetizuoti rizikas;*
4. *Identifikuoti kontrolės ir saugos priemones.*

1.5. ES platformų vertinimas ir pasirinkimas

Pirmosioms ES kurti buvo naudojamos LISP ir PROLOG programavimo kalbos. Kadangi darbo tikslas yra ES sistemos modelis, kuris turi veikti nepriklausomai nuo kitų sistemų, patiems kurti ES nėra prasmės. Kaip rašo Giarratano [13], jei problema negali būti išspręsta efektyviai tradiciniu programavimu, verta naudotis sukurtomis AI sistemomis.

Kuriant taisyklėmis pagrįstas ekspertines sistemas, ES apvalkalai tampa vis populiaresni. Ekspertinės sistemos apvalkalas yra lyg skeletas su pašalinta žinių baze. Norint sukurti naują ekspertinę sistemą, vartotojui reikia tik pridėti žinias taisyklių pagrindu ir pateikti tiesiogiai su žiniomis susijusią informaciją. Taip ekspertinių sistemų apvalkalai leidžia gerokai sumažinti ES kūrimo laiką [28].

Šiais laikais ES kuriamos populiaresnėms kalboms tokioms kaip JAVA, C, PYTHON, PERL, PHP. Kadangi ekspertinės sistemos kalba yra aukštesnio lygmens, ja atlikti numatytus darbus yra lengviau, tačiau yra apribojamos galimybės spręsti problemas, kurios yra neaprašytos. Su naujausiomis aplinkomis šitas apribojimas nebegalioja, kadangi galima reikiamas funkcijas vykdyti išėjus iš ES ir rezultatus gražinti į ją.

Tradicinės ES buvo skirstomos pagal aparatinės įrangos platformą, priklausomai nuo užduoties tipo, problemų sprendimo metodo. Dabartinės sistemos yra universalesnės, bet vis tiek išliko daug būdų joms charakterizuoti ir pasirinkimo kriterijams nusistatyti. Kalbant apie ES aplinkos pasirinkimą, kai yra bent kelios sistemos, kurios atitinka reikalavimus, ES knygų autoriai vieningai pataria išbandyti jas visas, sukuriant minimalų karkasą, taip tiksliau išsiaiškinant ES tinkamumą planuojamai sistemai.

Dabar ekspertinių sistemų kūrimo įrankių yra nemažai. Kadangi darbo tikslas yra ekspertinės sistemos veikiantis modelis, iš karto yra apsibrėžiamos sistemos ribos. Darbe nebus naudojamos senos sistemos nors ir patikrintos laiko, taip pat tos, kurių negalima išbandyti, nes jos išskirtinai komercinės.

Didesnis dėmesys skiriamas į tuos ES kūrimo įrankius, kurie yra nemokami arba nemokami mokymosi tikslams.

Nuspręsta, jog pagrindiniai kriterijai, pagal kuriuos įrankiai yra ieškomi, yra: **sistemos multiplatfromiškumas, naujumas, informacijos prieinamumas ir sistemos ateities tendencijos**.

Kaip ir minėta anksčiau, ES sistemų piko metu buvo kuriami ne įrankiai, o specializuotos ES tam tikra programavimo kalba. Kai kurios kompanijos buvo sukūrusios net po kelias sistemas, kurias skirdavo labai siaurai panaudojimo sričiai. Tokios aplinkos ar platformos, kaip pasirinkimas, atmestas iš karto dėl savo ne universalumo. Įrankių sąrašas, kurie atitinka keliamus reikalavimus, nėra didelis. Šiuo metu populiariausios nemokamos ES aplinkos yra: Clips, JESS, Drools. Komercinės: Exsys, PST, ILOG. Komercinės sistemos iš karto yra atmetamos, nes neturi net bandomosios versijos ir licencijos mokymuisi, bei yra orientuotos į galutinį vartotoją.

1 lentelė. Ekspertinių sistemų palyginimas

Ypatybė	CLIPS	JESS	DROOLS
Naujumas (taikomi sprendimai, formos, elementai)	-	x	x
Prieinamumas	x	x	x
Išvadų varikliuko algoritmas	RETE	RETE	RETE
Multiplatformiškumas	-	x	x
Žinių vizualizacija	-	-	x
Sistemos veikimo metodai	“Forward chaining”	“Forward/backward chaining”	“Forward chaining”
Modulinis taisyklių grupavimas	x	x	x

Iš aptartų sistemų ir išanalizuotų jų bendrų specifikacijų aiškią persvarą turintis įrankis yra CLIPS. Pirmoje lentelėje pateiktas populiariausių nemokamų ES kūrimo aplinkų palyginimas pagal nusistatytus kriterijus rodo, jog geriausiai sąlygas atitinka Drools, po jos seka JESS aplinka. Visgi šiame darbe nuspręsta pasirinkti JESS, taisyklėmis paremtą ES kūrimo aplinką, dėl jos populiarumo ir panaudojamumo pavyzdžių.

Nors CLIPS ir ekspertinės sistemos kūrimui išsirinktas JESS įrankis gali būti naudojami tiek su neraiškiąja logika, tiek su Būlio logika, šio darbo atveju labiau tinkamesnis yra Būlio logikos naudojimas. Taip nuspręsta dėl didesnio tokių sistemų išbaigtumo ir išanalizuotumo, išbandymų ir patvirtintų sprendimų. Nors egzistuoja teiginys, jos su neraiškiąja logika pagrįsta ekspertinė sistema gali tiksliau adaptuotis prie esamos situacijos, kuriant ES modelį, reikia papildomo projektavimo etapo, kurio metu būtų nuspręsta, kaip ir kieno pagrindu yra kuriami argumentavimo intervalai. Šiuo atveju reikėtų naudoti tam tikrą rizikos apskaičiavimo duomenų bazę, kurioje būtų susietas visas nagrinėjamas

įmonės turtas, grėsmės, naudojamos saugos ar rizikos mažinimo priemonės, apgalvoti galimus vertybių rinkinius. Norint sukurti tokią ES ir pasinaudoti visomis neraiškiosios logikos gerosiomis savybėmis, privalu būtų panaudoti ir tam tikrą duomenų susisteminimo metodą. Toks ES kompleksiškumas planuojamame darbe nereikalingas, be to, išeina ir už šio darbo ribų.

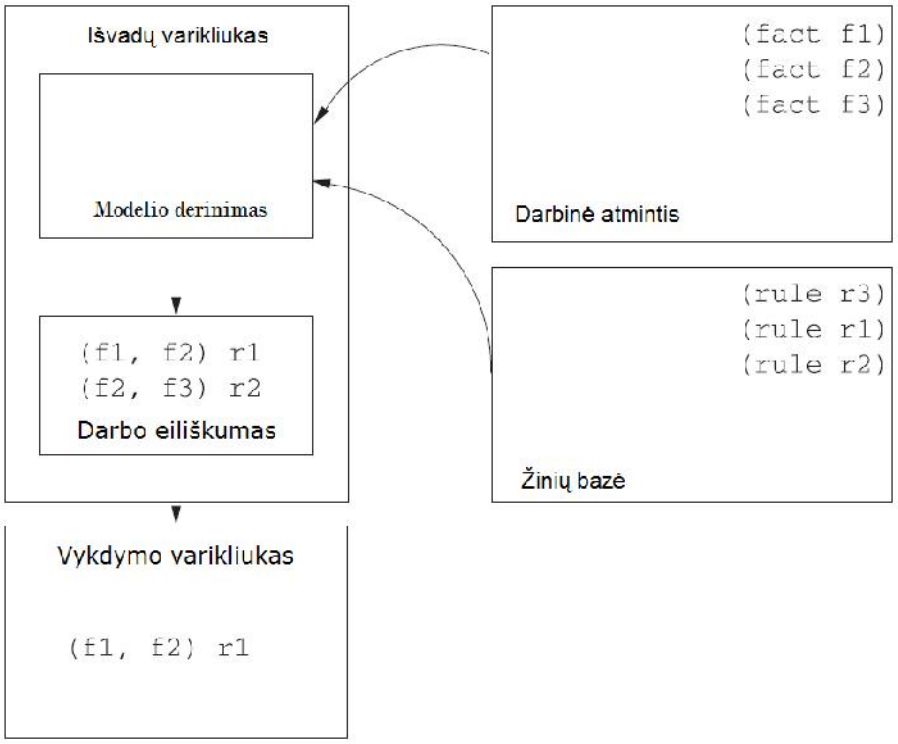
1.6. JESS ekspertinės sistemos platforma

Šiame skyriuje yra aptariami JESS sistemos komponentai ir jų funkcijos. Aprašomas su projektuojama ekspertine sistema susijusių komponentų taikymas ir jų subtilybės.

1.6.1. JESS architektūra

Dauguma šiuolaikinių ES išvadų varikliukų visgi yra daugiau ar mažiau specializuoti tam tikrai ekspertinei sistemai, kuri veikia tam tikroje aplinkoje ar yra programuojama ir pritaikoma tam tikrai sričiai. Todėl prieš pradedant analizuoti ES sistemos modelio kūrimą, yra būtina smulkiau išsiaiškinti išvadų varikliuko veikimą JESS aplinkoje. Bendrinio varikliuko komponentai buvo pavaizduoti pirmame paveiksle. Ketvirtame paveiksle yra schematiškai pavaizduoti ES komponentai, bei smulkiau išskirta, kas sudaro patį išvadų varikliuką. Trys išvadų varikliuką sudarantys elementai ir tuo pačiu diskretūs ciklo žingsniai yra tokie:

1. Visos taisyklės yra palyginamos su darbine atmintimi (naudojant modelio derintuvą), jog būtų galima nuspręsti, kurios taisyklės bus aktyvuotos ciklo metu. Toks sudarytas nerūšiuotas aktyvuojamų taisyklių sąrašas, kartu su kitomis taisyklėmis, kurios buvo aktyvuotos ankstesniais ciklais, vadinamas konfliktinių taisyklių rinkiniu.
2. Konfliktinių taisyklių rinkinys yra rūšiuojamas pagal taisyklių aktyvavimo eiliškumą, t.y. pagal taisykles, kurių dešinė pusė bus aktyvuojama. Toks rūšiavimo procesas yra vadinamas konfliktų sprendimas. Svarbiausia, jog konfliktų sprendimo strategija duotoms taisyklėms priklauso nuo daugelio veiksnių ir tik kai kurie iš jų gali būti kontroliuojami programuotojo.
3. Ciklas baigiamas, kai yra aktyvuojama pirmoji sąraše esanti taisyklė (aktyvuota taisyklė gali vėl iš naujo pakeisti darbinę atmintį) ir visas procesas kartojamas iš naujo. Toks pastovus ciklo kartojimas apima daug nereikalingo darbo. Tam, kad būtų efektyviau dirbama ir išvengiama perteklinių veiksmų, daugelis varikliukų naudoja sudėtingus greitinimo metodus. Pavyzdžiui, visų ciklų metu yra išsaugomi rezultatai, gauti po modelio derinimo ir darbo eiliškumo tvarkyklės, todėl aukščiau du aprašytus veiksmus reikia atlikti tik naujoms taisyklėms. Apie tai rašoma kitame poskyryje.



4 pav. ES komponentai [12]

Pradedantiems taisyklių programuotojams sunku sutikti su mintimi, kad taisyklių varikliukas nuspręs, kokia tvarka taisyklės bus aktyvuojamos, kas iš tikrųjų ir yra vienas iš didžiausių privalumų taisyklėmis grindžiamo programavimo. Taisyklių variklis sukuria daugiau ar mažiau skirtingą pasirinktinę programą kiekvienoje situacijoje skirtingai, tvarkant aukščiau minėtus derinius, kurių galbūt programuotojas nenumatė.

1.6.2. RETE algoritmas

Iš ankstesnio poskyrio ir teorinės medžiagos akivaizdu, kad standartinis modelio derinimo įgyvendinimas yra neefektyvus, kadangi kiekvienos taisyklės kairė pusė turi būti patikrinta su darbinėje atmintyje esančiais faktais kaskart po pasikeitimo. Aktyvavus viena taisyklę, visas darbas turi būti atliktas iš naujo, todėl taisyklių padvigubėjimas perpus sumažina sistemos efektyvumą. JESS vietoje standartinio modelio derinimo naudoja RETE algoritmą.

Pagrindinė RETE algoritmo mintis, jog besikeičiančios taisyklės ir faktai keičiasi skirtingu dažnumu. Tiksliau pastebėta, kad taisyklės keičiasi palyginti nedaug. Tai ir buvo panaudota kaip pagrindas efektyvinant taisyklėmis grindžiamų sistemų veikimą.

RETE algoritmas tapo pagrindu lengvai pagreitinti įvairias taisyklėmis pagrįstas sistemas. Egzistuoja ir RETE 2 algoritmas, kuris pritaikytas anksčiau minėtoje CLIPS aplinkoje. JESS aplinkoje jis nepritaikytas, o to priežastis - RETE 2 nėra viešai publikuojamas.

RETE algoritmas neefektyvumą modelio derinime pašalina įsimenant paskutinius pasikartojančius ciklo rezultatus. Tik nauji arba ištrinti darbinės atminties elementai yra testuojami, naudojant modelio derinimo funkciją. Taip pat RETE algoritmas modelio derinimą naudoja tik toms taisyklėms, kurių grupėms tie faktai galėtų atitikti. Tokiu būdu RETE algoritmas įgalina JESS atlikti greitą modelio derinimą.

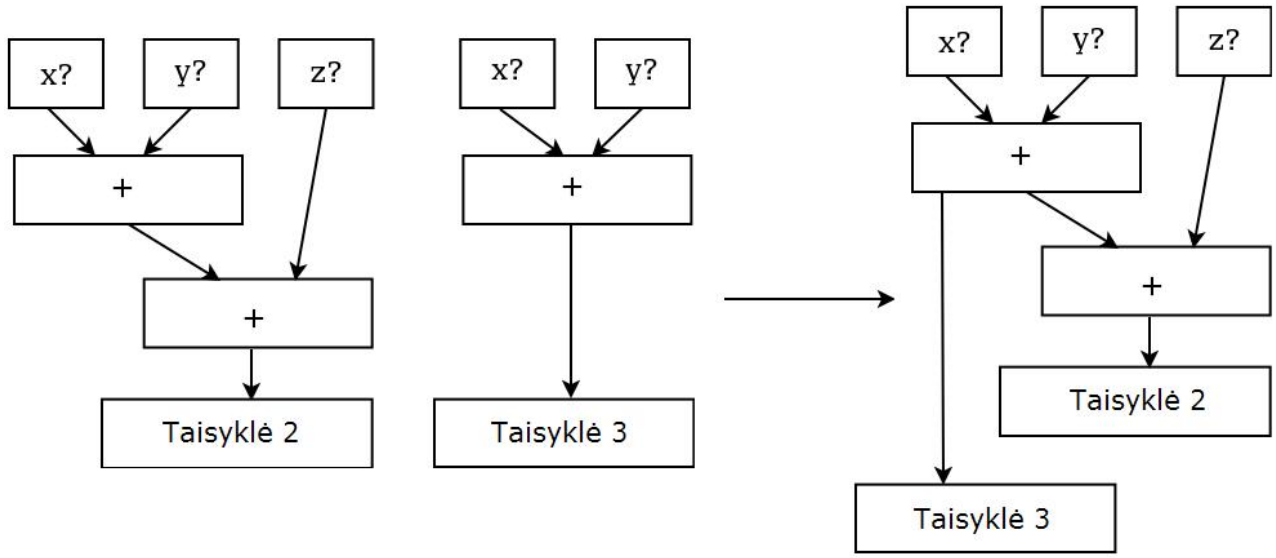
RETE algoritmas yra įgyvendinamas, sukuriant tarpusavyje sujungtų mazgų tinklą. Kiekvienas mazgas atstovauja taisyklės ar keleto taisyklių kairiajai pusei. Įvedami ar ištrinami faktai yra apdorojami šių mazgų tinklo. Tinklo viršuje yra įeinantys mazgai, o apačioje išeinantys.

Penktame paveiksle yra pateiktas RETE tinklo optimizavimo atvejis. Paveiksle matomi penki įeinantys mazgai, iš kurių tik trys yra skirtingi. Todėl galima pakoreguoti tinklą taip, kad dvi taisyklės dalintųsi trimis mazgais.

Diagramoje kiekvienas pavaizduotas keturkampis yra mazgas. Maži keturkampiai - vieno įėjimo mazgai, dideli keturkampiai - dviejų įėjimų. Iš mazgo išeina į kitą mazgą tik atitinkantys nurodytą modelį faktai.

Dviejų įėjimų mazgai prisimena visus faktus ar jų grupes, kurie ateina į vieną iš įėjimų, taip pat kuria dviejų ar daugiau faktų grupes optimizavimui išėjime. Faktai įeinantys mazgo kairėje ir dešinėje segmentuojami atskiruose atminties blokuose.

Ir galiausiai, tinklo apačioje esantys mazgai atspindi individualias taisykles. Jie turi tik vieną įėjimą ir jokių išėjimų. Gavus mazge įėjimą, yra įrašomas aktyvavimo įrašas, po kurio taisyklė keliauja į darbo eiliškumo elementą.



5 pav. RETE tinklo optimizavimas [12]

RETE algoritmas keitėsi laikui bėgant, priklausomai nuo sistemų tobulėjimo ir poreikio paraleliniam ir daugiaprocesoriniam efektyvumui. RETE kūrėjas Charles Forgy atnaujinto RETE2 algoritmo veikimo nepateikė, pateikdamas tik faktus, kad RETE2 yra greitesnis kompleksiškose

problemose. Yra ir daugiau RETE versijų, bet jų veikimas nepublikuotas, esti tik patys faktai apie jų egzistavimą.

1.6.3. Faktai JESS aplinkoje

Prieš pradedant analizuoti patį ES sistemos projektavimą, yra svarbu išsiaiškinti JESS aplinkos taisyklių ir faktų kūrimo aspektus.

Faktai yra laikomi darbinėje atmintyje, dar kitaip vadinamoje faktų bazėje, kas jau yra žinoma iš ankstesnio skyriaus. Darbinėje atmintyje yra laikomi tiek pradiniai faktai, tiek ir faktai, gauti aktyvavus taisykles. Tam, kad talpintų ir greitai pasiektų faktus, JESS naudoja individualių indeksų rinkinį, pagal principą, panašų į naudojamą reliacinėse duomenų bazėse. Kiekvienas faktas yra saugomas darbinėje atmintyje tokiu eiliškumu kaip ir buvo patalpintas.

Faktai darbinėje atimtyje gali būti nerūšiuoti ir rūšiuoti. Nerūšiuoti faktai - tai duomenų struktūra, kai viena duomenų eilutė yra padalinta ląstelėmis, kiekvienoje ląstelėje įrašant atskiro tipo ar reikšmės informaciją. Įterpiant nerūšiuoto tipo faktą prieš tai yra sukuriamos ląstelės, kuriose bus talpinami duomenys. Rūšiuoti faktai - tai duomenų struktūra, kuri atrodo tiesiog kaip sąrašas duomenų, atskirtų tarpais vienoje eilutėje. Dažniausiai naudojami nerūšiuoti faktai. Būtent tokio tipo faktai ir bus naudojama šiame darbe projektuojant ES.

1.6.4. Taisyklės JESS aplinkoje

Taisyklės gali imtis veiksmų, remiantis darbinės atminties turiniu. Darbinė atmintis tiesiogiai pasiekiama per užklausas. Užklausos ieško darbinėje atmintyje konkrečių faktų ir nagrinėja jų sąryšius. Užklausos yra labai panašios į taisykles, todėl taisyklę galima lengvai paversti užklausa ir atvirkščiai.

Kadangi taisyklėmis pagrįsta sistema gali turėti šimtus taisyklių, tikėtina, kad bet kuriuo metu daugiau nei viena taisyklė gali būti aktyvuota. Suaktyvėjusių taisyklių, kurios gali būti aktyvuotos, rinkinys, kaip minėta aukščiau, yra vadinamas konfliktų rinkinys. Konfliktą JESS valdo, naudojant konfliktų sprendimo strategijas (*angl*. conflict-resolution strategies). JESS turi dvi strategijas: gylio (*angl*. depth) (pagal nutylėjimą) ir pločio (*angl*. breadth). Naudojant gylio strategiją, pirmiausia aktyvuojamos pastaruoju metu aktyvuotos taisyklės, o pločio strategiją - pirmiausiai aktyvuojamos seniausiai aktyvuotos taisyklės. Strategijų keitimo dažniausiai prireikia, kai numatytosios strategijos naudojimo metu kiekviena aktyvuota taisyklė aktyvuoja dar vieną taisyklę ir taip pasikartoja ciklišKai. Tuomet seniausiai aktyvuotos taisyklės lieka neaptarnautos.

Kita galimybė valdyti taisyklių aktyvavimą yra taikyti taisyklės prioritetą (*angl*. salience). Kiekvienai taisyklei galima pritaikyti taisyklės prioritetą. Tokiu atveju, taisyklės aktyvuojamos pagal prioritetą nuo didžiausio iki mažiausio. Jeigu kelios taisyklės turi vienodą prioritetą, jų aktyvavimo eiliškumas nusprendžiamas pagal konfliktų sprendimo strategiją, kaip aprašyta ankstesnėje pastraipoje.

Prioritetą galima nurodyti skaitine reikšme, globaliu kintamuoju. Prioritetą taisyklei galima priskirti rankiniu būdu arba nurodžius, jog jis būtų priskirtas aktyvinus tam tikrą taisyklę ar ciklą. Kadangi prioritetai labiau naudojami procedūrinėse kalbose, JESS aplinkoje piktnaudžiauti prioritetais neverta, kadangi tai turi neigiamą poveikį spartai ir gali lemti neteisingą taisyklių aktyvavimą.

Dar vienas būdas spręsti didelių taisyklių bazių problemas yra jų skaidymas į gabaliukus. Naudojant „*defmodule*“ galima taisykles ir faktus padalinti į, taip vadinamus, modulius. Modulių naudojimas yra teigiamas veiksmas dėl kelių priežasčių: loginio grupavimo bei taisyklių aktyvavimo tik iš aktyvaus taisyklių modulio. Kontroliuojant modulius galima valdyti programos vykdymą. Taisyklė gali būti iššauta (*angl.* fire) tik tame modulyje, kuris yra tuo metu aktyvus. Modulius galima aktyvuoti nurodyta tvarka. Taip pat galimas variantas - automatinis modulio aktyvavimas programos paleidimo metu.

Šiame darbe projektuojama ekspertinė sistema taip pat yra suskirstyta moduliais, kurie aprašyti sekančiame skyriuje. Moduliai aktyvuojami paeiliui, aiškiai apibrėžiant sistemos vykdymo etapus.

2. ES modelio kūrimas ir bandymai

Kadangi ES modelis bus kuriamas naudojant JESS aplinką, daug įprastų projektavimo etapų, kaip kuriant informacines sistemas ar programinę įrangą nebus naudojama. Šios ekspertinės sistemos modelio projekte aprašomi funkciniai ir ekspertinės sistemos struktūriniai reikalavimai.

2.1. ES modelio projektas

Kaip aukščiau paminėta, pasirinkus JESS ekspertinės sistemos kūrimo aplinką, toliau išvardinti kūrimo etapai, kurie yra visai neaktualūs, kuriant aptariamą ES: saugos specifikacijos, vartotojo sąsajos, duomenų apdorojimo ir duomenų bazės reikalavimai, diegimas ir jo reikalavimai, vartotojo dokumentacija, programos architektūra, komponentų tarpusavio elgsena, duomenų srautai, aparatūriniai ir programiniai reikalavimai.

Kuriamai ekspertinei sistemai būtina aprašyti funkcinius ir struktūrinius sistemos reikalavimus. Žinių bazė, jos veikimas ir programos veikimo eiliškumas aptariamas taisyklių ir faktų poskyryje. Sistemos vartotojo sąsaja standartinėje JESS aplinkoje yra paprasta ir pakankama aptariamam ekspertinės sistemos modeliui.

2.1.1. Funkciniai reikalavimai

Funkciniai reikalavimai ekspertinei sistemai yra šie:

1. Ekspertinė sistema turi apimti mikro, mažos ir vidutinės įmonės informacijos saugos klausimus.
2. Sistema turi būti paprasta ir jos pateikiami klausimai turi būti suprantami visiems vartotojams, turintiems bazines IT saugos žinias.
3. Sistema faktus sužino iš vartotojo pateiktų atsakymų į užduotus klausimus.
4. Vartotojas turi turėti galimybę keisti faktus, paimtus iš dinaminės faktų bazės ar įrašydamas dalį faktų iš jau gauto ES sistemos pateikto XML rezultatų failo.
5. Pateikiami klausimai turi būti aktualūs tik pradžioje programai nurodytam įmonės profiliui.
6. Sistemos pateikiami rezultatai yra išvedami į ekraną ir į XML failą.
7. Į sistemos pateikiamus klausimus atsakyti galima tik riboto tipo ir variantų atsakymais.
8. Jeigu kuri nors svarbi informacija nepakliūna į rizikos vertinimo procesą, sistema tą reikšmingą informaciją pateikia rekomendacijų pavidalu, po rizikos analizės rezultatų.

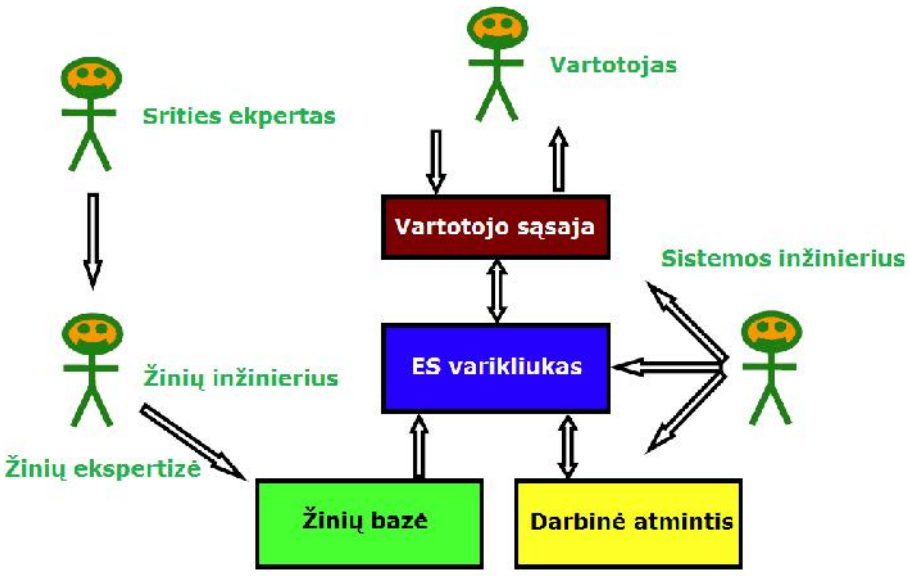
Reikėtų paminėti, jog vartotojas turi turėti galimybę nurodyti toleruojamos rizikos reikšmę. Tolerancijos lygmuo šiuo atveju sistemoje yra svarbus ne tik rizikos vertinime, o ir galimybei ES sistemą panaudoti kaip priemonę, analizuojant kaip keisis rizikos vertės ką nors įmonėje keičiant ar tiesiog aiškinantis, ar į rizikos vertinimą nepakliuvo ribinės reikšmės.

Sistemos rezultatų pateikimo reikalavimai:

1. Sistema, pateikdama rezultatus, pateikia tik tas vertybes, kurių apskaičiuota rizikos vertė yra lygi arba didesnė nei nurodyta toleruojama.
2. Sistemos pateikiamuose rezultatuose kiekviena vertybė, kurios rizika yra lygi arba viršija nurodytą toleruotiną, išskiriama atskirai.
3. ES pateikiant apskaičiuotą vertybės rizikos reikšmę, pateikia ir tikimybės reikšmę, kuri buvo panaudota rizikos skaičiavimui.
4. Pateikiant rizikos vertę, yra pateikiama tokios apskaičiuotos rizikos priežastis ir galimi rizikos mažinimo variantai ar naudotinos priemonės.

2.1.2. Ekspertinės sistemos struktūra ir žinių bazė

Standartinė ir visur naudojama kaip etaloninė ES struktūra pavaizduota šeštame paveiksle.

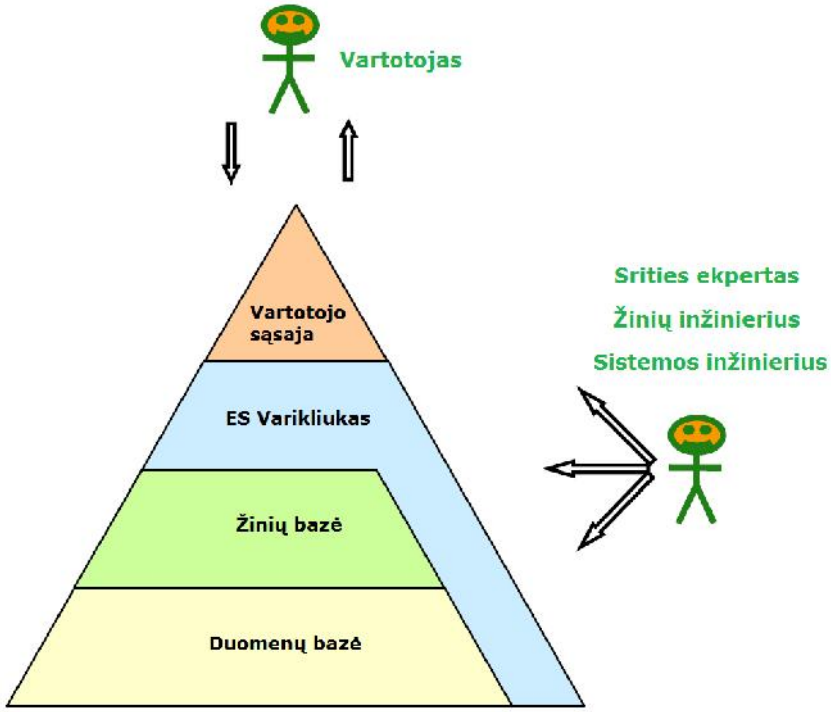


6 pav. Standartinė ES struktūra ir dalyvaujantys aktoriai [40]

Ši struktūra darbe yra tinkama tik iš dalies dėl kelių priežasčių.

1) Kuriamo ES modelio atveju, dėl darbo specifikos ir apimties tokie aktoriai kaip sistemos inžinierius, srities ekspertas ir žinių inžinierius bus pakeisti vienu aktoriumi – žinių inžinieriumi.
2) Be žinių bazės aptariamoje ES bus naudojami faktai iš dinaminės faktų bazės.

Dėl sistemos specifikos ir poreikio taikyti kintančius faktus, kurie būtų pateikiami iš dinaminės faktų bazės, nuspręsta žinių bazę ir duomenų bazę struktūrizuoti kaip pavaizduota septintame paveiksle.



7 pav. Kuriamos ES struktūra ir aktoriai

Tokiu būdu, jeigu yra naudojami faktai iš dinaminės faktų bazės, jie yra patalpinami atmintyje kaip aukštesnio prioriteto faktai ir sistema nebeužduoda klausimų, norint tuos faktus sužinoti. Jeigu sistemoje iššauna taisyklė, kuri turėtų keisti jau iš faktų bazės paimtą faktą, ji to fakto nebekeičia. Priešingu atveju, jeigu sistema nenaudoja faktų iš išorinės faktų bazės, visi sistemai reikalingi faktai sužinomi iš vartotojo ar atitinkamai iššovus tam tikroms taisyklėms.

Ekspertinės sistemos žinių bazė JESS aplinkoje aptariamai sistemai yra tinkama be papildomų reikalavimų. Duomenų bazei ES atžvilgiu yra svarbu XML failo struktūra ir tuščių faktų nebuvimas, kuris gali iškraipyti ES pateikiamus rezultatus.

2.2. Saugos valdymas ir rizika

Bendri saugos valdymo klausimai ES yra panaudoti iš geryjų rizikos vertinimo praktikų. Klausimai yra skirti vidutinio dydžio įmonių rizikos vertinimui arba įmonėms, kurios nori įvertinti riziką pagal ISO standartą, yra sudaryti pagal ISO 27K dokumento A priede pateiktų klausimų lentelę, kurioje nurodyti saugos kontrolės tikslai ir priemonės. ISO 27K dokumentas pasirinktas kaip klausimų šaltinis ES žinių bazės pildymui, kadangi tai vienas iš svarbesnių, paremtas tarptautinių saugos valdymo praktikų, dokumentų. Klausimai sistemoje patalpinti tokiu pat eiliškumu kaip ir pateikta

dokumente, bet jų pateikimas vartotojui priklauso nuo pateiktų atsakymų, tai yra, priklauso nuo taisyklių ir faktų. Dalis ekspertinės sistemos naudojamų klausimų yra pateikta pirmame priede.

Rizikos analizės ir vertinimo procesu yra efektyviai padedama organizacijos operacijoms, identifikuojant rizikas, kurioms reikia savininkų ar valdytojų dėmesio, kas ir yra šios ES tikėtini naudotojai. Rizikos analizę ekspertinėje sistemoje sudarys dvi pagrindinės dalys: šaltinio nustatymas ir rizikos apskaičiavimas. Rizikos analizės rezultatai sukuria pagrindą rizikos vertinimui, rizikos valdymui ir rizikos priėmimui. ES, pateikdama rezultatus ar patarimus valdytojams ar savininkams, pateiks juos pagal rizikingumą. Kontrolės veiksmai ir kaštų – naudos analizė nebus pateikiama, nes tai yra per daug kintama ekspertinės sistemos atžvilgiu.

Kiekybinės analizės metu rizikos lygis nurodomas skaitine verte, atitinkančia jos parametrų pasekmių ir tikimybės dydžius. Naudojant kiekybinę analizę, galima numatyti atskirų rizikų ir viso tyrimo rizikos kiekybinę vertę, kas yra aktualu šios sistemos rėmuose. Kalbant apie mažas įmones, reikėtų paminėti, jog taikant kiekybinį atskirų galimų rizikų ir pasekmių įvertinimo būdą, galima išskirti labiausiai tikėtinas rizikas, kurios gali sukelti svarbius praradimus mažiems verslo vienetams.

Svarbią informacijos valdymo dalį užimanti rizikos analizė ir jos valdymas ES bus išreikšta kiekybiniais parametrais. Kiekybinė rizikos analizė šios projektuojamos ES mastu yra pakankamai išsami. Ji konstruojama taip, kad būtų kiekybiškai įvertinti komplikuoti ir įvairūs rizikos scenarijai. Atliekant kiekybinę rizikos analizę bus, naudojamas keturių žingsnių metodas.

Projektuojamoje ES rizikos analizė atliekama sekančiais etapais:

1) Identifikuojamas turtas ar vertybė;
2) Aiškinamasi kylančios grėsmės identifikuotam turtui ar vertybei;
3) Įvertinamas turtas ar jo svarba kuriam kyla grėsmės;
4) Nurodomos naudojamos saugos priemonės rizikos mažinimui.

Atlikus egzistuojančios grėsmės rizikos analizę, kurių vertės yra nepriimtinos, yra pateikiami tikėtini rizikos mažinimo kaštai. Jeigu iš esamų faktų esančių atmintyje rezultatai yra aiškūs, papildomi klausimai nebeužduodami. Jeigu klausimai užduodami, bandoma išsiaiškinti iki tam tikro tikslumo, kadangi kiekybinės analizes metu grėsmes, rizikas, mažinimo kaštus išanalizuoti išsamiai reikia kelis kartus daugiau informacijos nei kokybinės analizės atveju. To atsisakyta, kadangi tai išeina iš šio darbo ribų.

Efektyvus rizikos valdymas užtikrinamas tik nuolatos taikant nuolatinės rizikos analizės metodą. Kadangi rizikos analizė turi tiksliai atitikti aplinkos pobūdį, kas ir kokio tipo nagrinėjama, kas yra ir ko nėra, nuspręsta rizikos analizę taikyti po bendrų ES pateikiamų klausimų. Tai turėtų leisti

pateikti efektyvesnius atsakymus-patarimus, kuriais pasinaudojant būtų galima sumažinti nepriimtiną riziką iki priimtino ar leistino lygio.

Rizikos vertinimo etapas atliekamas atskiru moduliu sistemoje. Išrenkamas grėsmių turintis vertinamas turtas, užduodami papildomi klausimai apie jį, lyginami esami faktai su tikėtinais. Vertinimo metu remiamasi eksperto įvestais statistiniais duomenimis arba duomenų bazės žiniomis.

Rizikos vertinimas atliekamas pagal antroje lentelėje pateiktą vertinimo matricą. Rizikos vertinimo matricos šaltinis yra ISO 27005 standartas.

2 lentelė. Rizikos vertinimo matrica [18]

Turto vertė	0	1	2	3	4
Tikimybės vertė					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Rizikos vertinimo rezultatas tai turto vertės ir tikimybės įvykti grėsmei, verčių suma. Ji kinta nuo mažiausios reikšmės nulio iki didžiausios - aštuonių.

2.3. Taisyklės ir faktai

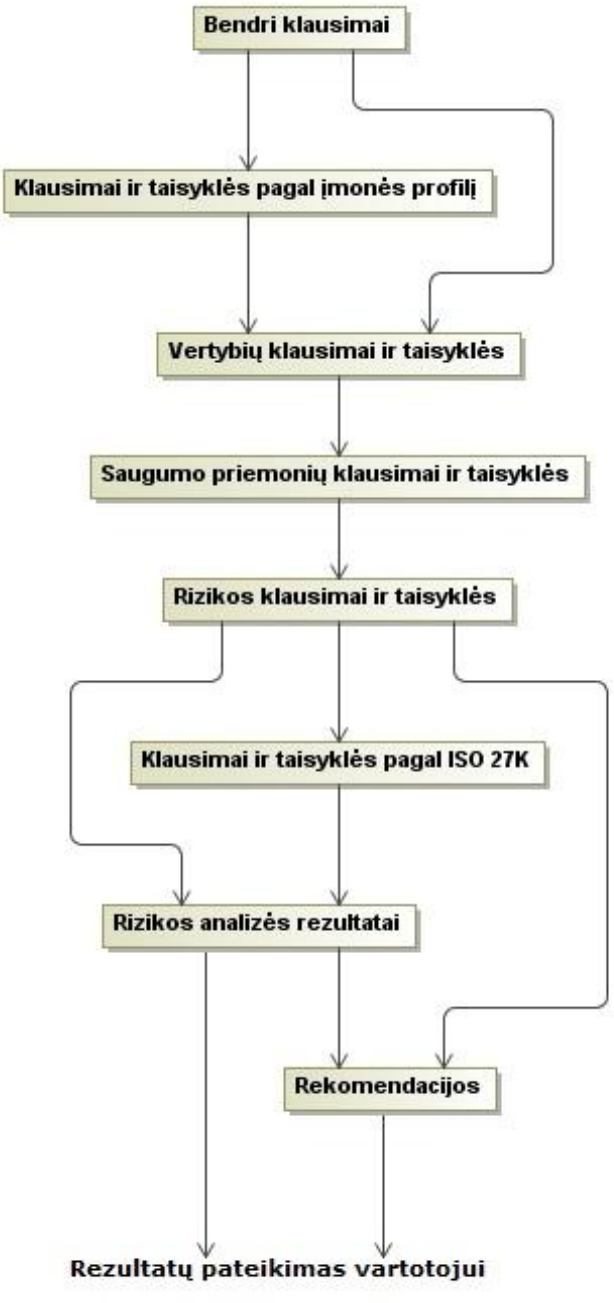
Taisyklės ir faktai, kaip jau anksčiau minėta, laikomi žinių bazėje, o faktai kuriamoje ES gali būti dar ir duomenų bazėje kaip failas arba dinaminėje faktų bazėje. Faktai pateikiami ir išsaugomi į XML failą. Išsaugotą XML failą galima prisitaikyti pagal poreikius. Faile pateikiami faktai iš dinaminės faktų bazės neaptariami, kadangi tai yra atskira tema, kaip gauti struktūrizuotas tikimybes arba įžvalgas iš tam tikrų šaltinių.

Ekspertinėje sistemoje įmonės dydžio apibrėžtis pritaikyta pagal Europos Sąjungos 2003/361 rekomendaciją. Kuriamoje ekspertinėje sistemoje įvesti penkių skirtingų įmonių profiliai: elektroninės komercijos, programavimo, dizaino, transporto ir medicinos kabineto. Priklausomai nuo įmonės profilio, yra pateikiami specialūs klausimai, kurie aktualūs tik nurodyto profilio įmonei.

Tam, kad būtų lengviau pritaikyti ekspertinę sistemą skirtingo dydžio ir profilio įmonėms, nuspręsta klausimus ir taisykles grupuoti. JESS ekspertinėje sistemoje tai padaroma išskaidant norimus klausimus ir taisykles į modulius. Moduliuose esančios taisyklės ir faktai gali iššauti tik modulio aktyvumo metu. Jei taisyklė yra aktyvuojama, kai modulis neaktyvus, taisyklė neiššauna. Todėl svarbu apgalvoti modulių aktyvavimosi tvarką ir taisyklių išdėstymą. Priimtas sprendimas kaip išdėstyti modulius, yra pavaizduotas aštuntame paveiksle. Paveiksle pateiktoje diagramoje keturkampis

vaizduoja ES modulį, o rodykle nurodomas modulis, kuris bus aktyvuotas sekantis. Sekančio modulio aktyvacija yra sąlyginė ir priklauso nuo prieš tai esančio modulio gautų faktų ir iššautų taisyklių. Vienu metu galimas tik vienas modulio aktyvumas. Modulių aktyvacija galima tik viena kryptimi, kaip pavaizduota diagramoje. Antrame priede yra pateikta dalis ekspertinėje sistemoje taikomų taisyklių.

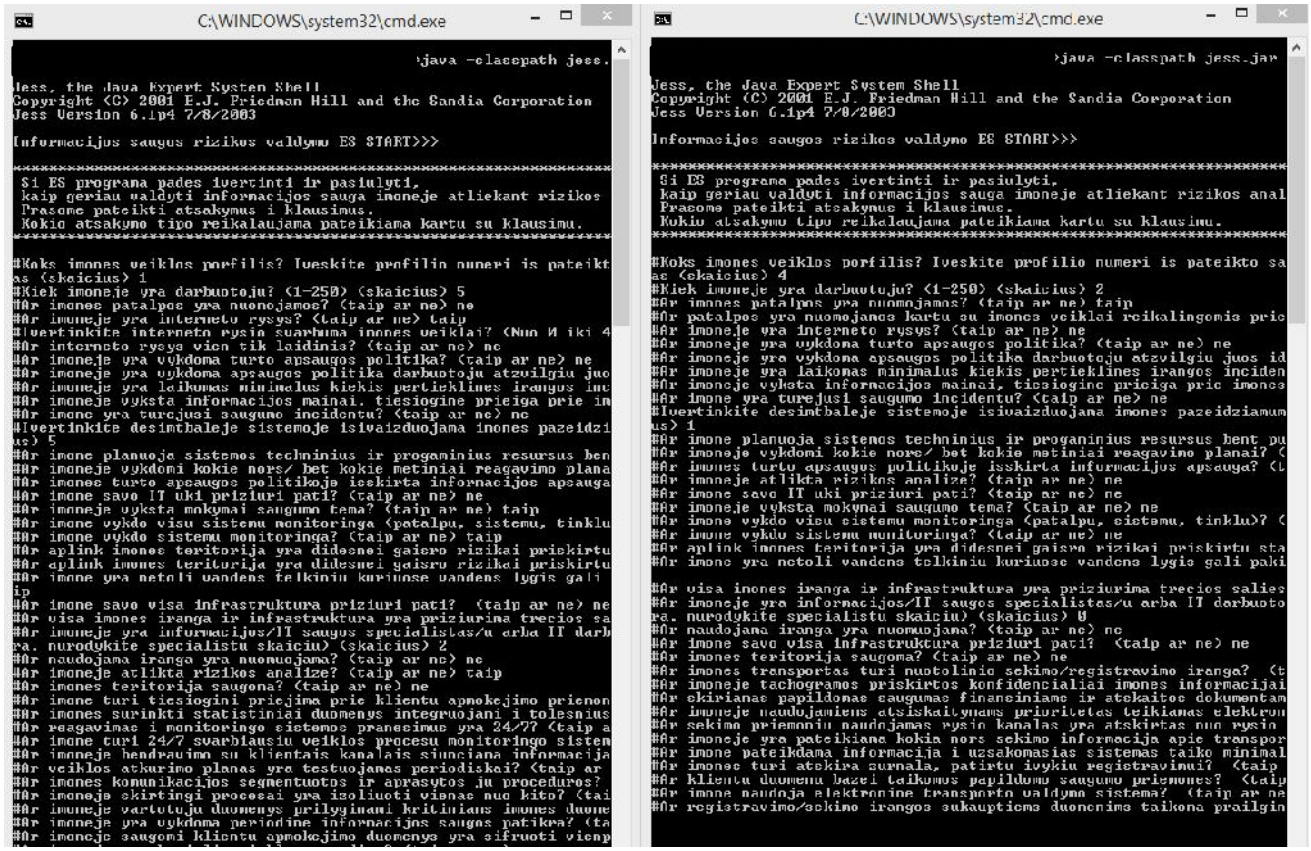
ES pradeda veikti, pateikdama trumpus nurodymus vartotojui, ir iš karto po jų seka bendri klausimai. Bendrų klausimų atsakymai, kaip faktai, lemia tolesnių taisyklių iššovimą. Bendrų klausimų metu gauti faktai daugiausiai ir lemia tolesnių taisyklių aktyvaciją, lyginant su kitų modulių klausimais. Kadangi nuo bendrų klausimų taisyklių daug kas priklauso, jos kuriamos taip, kad po jų prieštaraujančių faktų sistemoje negalėtų būti.



8 pav. ES moduliai ir jų aktyvacijos eiliškumas

Pagrindiniai faktai, kurie toliau nulemia sistemos pateikiamus klausimus, yra įmonės profilis, įmonės dydis, saugos politika. Priklausomai nuo pateiktų faktų, pagal įmonės profilį yra aktyvuojamos taisyklės. Jeigu profilis nenurodytas arba ekspertinėje sistemoje toks neaprašytas, yra aktyvuojamas vertybių identifikavimo modulis. Po jo seka saugumo priemonių modulis. Išsiaiškinus naudojamas saugos priemones, yra aktyvuojamas rizikos klausimų modulis. Priklausomai nuo to, koks buvo pasirinktas įmonės profilis ir įmonės dydis, toliau yra aktyvuojamas papildomų klausimų pagal ISO 27K modulis. Jeigu ISO klausimų modulis neaktyvuojamas, toliau aktyvuojamas rizikos analizės arba rekomendacijų modulis. Priklausomai kas buvo aktyvuota prieš tai, aktyvuojamas sekantis modulis arba ES baigia darbą. Tokiu būdu veikia darbe aprašomos ekspertinės sistemos modulių aktyvacija.

Devintame paveiksle pateikti du ekspertinės sistemos langai. Juose vaizduojama sistemos skirtingų klausimų uždavimas pateikus skirtingus faktus.



9 pav. ES modelio langas

Languose taip pat matoma, jog vartotojo sąsaja yra tekstinė, kur kiekvieno klausimo metu yra pateikiama, kokio tipo ir rėžių duomenų pageidaujama.

2.4. ES testavimas

Kaip mini ekspertinių sistemų autoriai, kuo platesnis problemos aprašymas taisyklėmis, tuo didesnis atsakymų tikslumas, kas nebūtinai teisinga žmonių atveju, kas ir buvo jau minėta ankščiau

[10]. Todėl neišvengiamai tokiai sistemai yra reikalingas automatinis testavimas, kuris teoriniu požiūriu turėtų apimti beveik visus galimus taisyklių ir faktų derinius, o realiu požiūriu apimtų kuo didesnį visų galimų variantų skaičių, kadangi ekspertinė sistema rodo dirbtinį intelektą. Taip pat pradėjus testuoti kuriamą programą ankstyvuosiuose etapuose, galima išvengti kelių lygių klaidų, kurias palikti ES yra labai paprasta, o norint jas ištaisyti, tektų rašyti naujas konfliktus sprendžiančias taisykles.

Pats JESS autorius siūlo testavimui naudoti JUnit testavimo aplinką, bet vėliau pripažįsta, jog JESS reikalingas ne procedūrinis kodo testavimas, o deklaratyvus, todėl norint atlikti menkiausią testavimą, tektų JUnit sukurti sudėtingą programą paprastam, kelių tipų bei reikšmių, automatiniam atsakymų pateikimui. Kadangi darbo pradžioje nuspręsta dirbti tik JESS aplinkoje, nenaudojant JESS pagrindu kurtos JAVA aplikacijos, JUnit testavimo atsisakyta. JUnit aplinką vertėtų naudoti jei visa ES būtų perkelta į JAVA, tuomet, naudojant klases, butų galima paduoti atsakymus tiesiog klasių pavidalu.

Statinis ES testavimas atliekamas ES kūrimo stadijoje ir yra mažesnės apimties nei dinaminis testavimas, apimantis taisykles ir faktus. Todėl buvo nuspręsta išbandyti automatizavimui skirtas programas, tokias kaip Expect, AutoIT, ActiveState ActiveTcl, kadangi ES testavimas didžiąja dalimi yra dinaminis taisyklių ir pateiktų rezultatų tikrinimas. Paaiškėjo, jog planas automatizuoti atsakymų pateikimą į ES pateikiamus klausimus su minėtomis programomis yra gana komplikuotas. Kadangi JESS veikia JAVA pagrindu, su minimomis programomis norint atlikti elementarius veiksmus, reikia įdirbio, nors ir po jo rezultatai vis tiek neatitinka lūkesčių. Kita aukščiau minėtų programų blogoji savybė – ne visos jos veikia LINUX operacinėje sistemoje.

Galutinėje testavimo įrankio pasirinkimo stadijoje buvo nuspręsta automatinį testavimą išskirti į dvi dalis: automatinį atsitiktinį ir automatinį tikslinį. Automatinio atsitiktinio testavimo metu ES modelio veikimas ir jo pateikiami rezultatai yra testuojami atsitiktinėmis reikšmėmis, o automatinio tikslinio testavimo metu iš pradžių ES yra pateikiami pageidaujami faktai ir tik po to atsitiktiniai atsakymai. Testuojant automatinio tikslinio testavimo metu iš pradžių pateikiami norimi faktai, kuriais galima lemti toliau ES pateikiamus klausimus ir galutinius rezultatus. Taip testuojant galima lengvai atrasti pastebėtas klaidingas taisykles.

Atliekant abiejų tipų testavimą yra įjungiamas faktų, taisyklių ir jų aktyvavimosi stebėjimas, kad būtų galima patikrinti, kas ir kokį taisyklės iššovimą nulėmė.

2.4.1. Automatinis atsitiktinis

Automatiniam atsitiktiniam testavimui nuspręsta pasinaudoti standartiniais Linux CLI įrankiais ir visą tai įkomponuojant į „bash“ skriptą. Visa testavimo procedūra nedokumentuojama. Išsaugomi

tik testų žurnalai-ataskaitos ir JESS pateikiamas faktų ir taisyklių XML failas, kurie skirti vėlesnių peržiūrų galimybėms.

Atsakymų failui generuoti galima naudoti LINUX „seq“ ar paprasčiausią Excel lentelę. ES testavimo atveju atsakymų failas buvo sugeneruotas naudojantis EXCEL lentele, kurioje dviejų tipų atsakymai, nes šiuo metu ES priima tik dviejų tipų atsakymus: tekstinius atsakymus tik „taip“ arba „ne“ ir skaitines vertes. Tokio failo panaudojimas testavimui tuo pačiu patikrina ir ar ES priima atsakymus teisinga forma kuri nurodyta klausime.

Testavimas susideda iš keturių dalių: sugeneruotų atsitiktinių atsakymų maišymas, programos paleidimas ir neinteraktyvus atsakymų pateikimas iš failo kuriame sumaišyti atsakymai, neapdorotos ataskaitos išsaugojimas, ataskaitos apdorojimas ir išsaugojimas į programos pradžioje nurodytą failą. Dešimtame paveiksle pateikiamas „b.sh“ skripto išeities kodas.

```
echo "Iveskite ataskaitos pavadinima"   #ataskaitos pavadinimo prasymas
read atas                               #ataskaitos failo nurodymas
echo "Ataskaitos failas" $atas".txt"    #pilnas ataskaitso pavadinimas
shuf rand.txt >rand1.txt                #maisomas sugeneruotu atsakymu failas
java.exe -classpath jess.jar jess.Main ESv2.clp < rand1.txt > ats.txt   #ES
paleidimas
sed '1,14d' ats.txt >atas.txt           #programos informacijos trinimas is
ataskaitos
sed 's/#/\n&/g' atas.txt >ats.txt       #ataskaitos skaidymas eilutemis
sed -i -e '1d' ats.txt                  #pirmos tuscios eilutes trinimas
pr -tmJ ats.txt rand1.txt > atas.txt    #taisykliu ir atsakymu formatavimas i
ataskaita
awk '$2>="$$$$"' atas.txt > "$atas".txt#ataskaitos irasymas i faila
awk '{a[$4]=$0} END {for (i in a) print a[i]}' "$atas".txt >atas.txt #pertiekliniu
eiluciu salinimas
sed -i -e '$a\' "$atas".txt             #naujos eilutes iterpimas
sed -i.bck '$s/$/~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~/' "$atas".txt #ataskaitu
atskyrimas
sed '1!G;h;$!d' atas.txt >>"$atas".txt #
read -p 'Testas baigtas'         #EOB
```

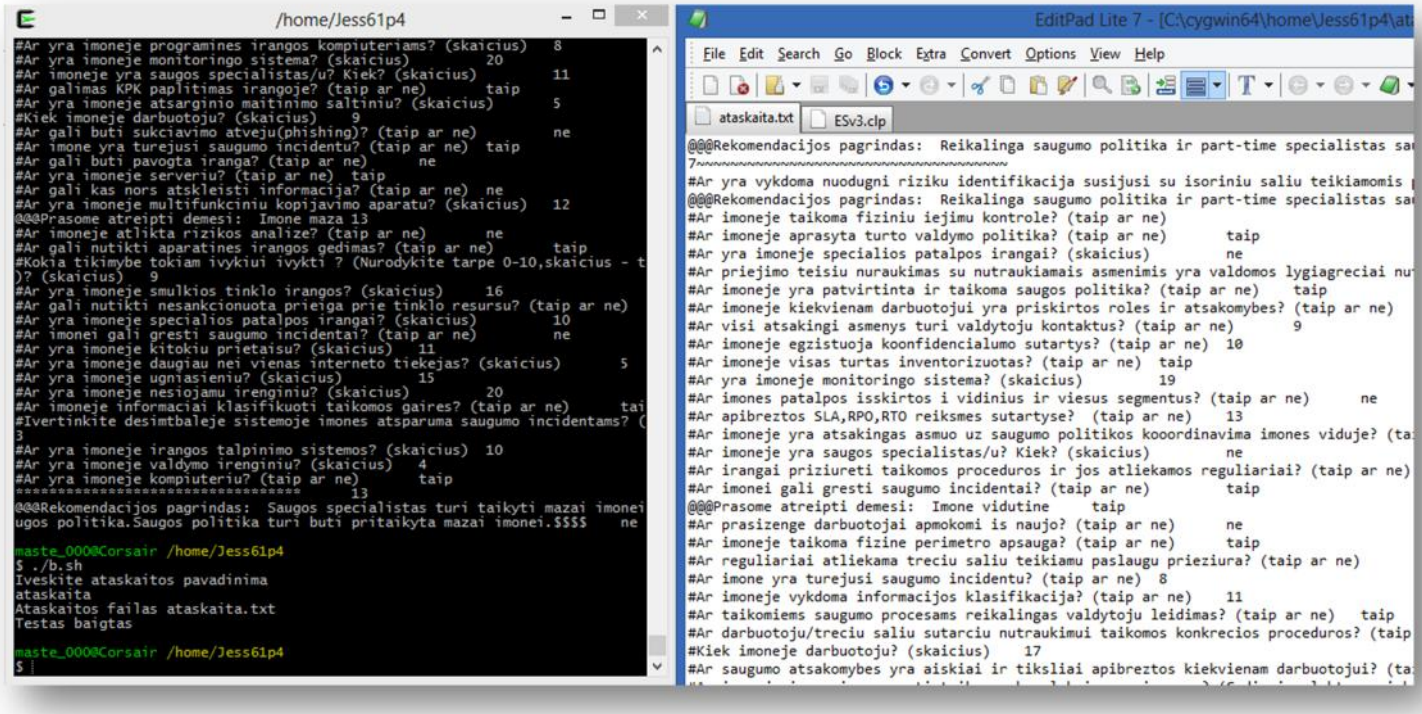
10 pav. ES automatinio testavimo skriptas

Sekančiame poskyryje, vienuoliktame paveiksle, pavaizduoti testavimo procesas ir pateiktos ataskaitos turinys.

2.4.1. Automatinis tikslinis

Automatinis atsitiktinis testavimas yra labai patogus būdas testuoti visas taisykles ir visos ES veikimą. ES pildant naujomis taisyklėmis ar jas tikslinant, toks automatinis atsitiktinis testavimas yra neefektyvus. Tokiems testavimams nuspręsta taikyti automatinį tikslinį testavimą. Lyginant su automatiniu atsitiktiniu, jis skiriasi tuo, jog testuojant iš pradžių yra pateikiami konkretūs testavimui skirti faktai ir tik jų trūkstant yra toliau tęsiamas testavimas naudojant atsitiktines faktų reikšmes.

Faktai sistemai yra pateikiami naudojant XML faktų failą, kuris yra nuskaitomas, pradedant veikti ekspertinei sistemai, arba pasinaudojus taisyklėmis, įrašant faktus tiesiai į ekspertinę sistemą, kas yra labai nepatogu ir didina klaidų tikimybę.



11 pav. ES testavimas

Nurodant iš karto reikiamus faktus, galima ištestuoti kiekvieną taisyklę atskirai arba tik dalį jų, tolesnį testavimą atliekant naudojantis atsitiktinėmis reikšmėmis. Ekspertinei sistemai gavus faktus, klausimai, kurie yra skirti tų faktų gavimui, nebėra užduodami, nebent iššauna tikslinančioji taisyklė. Aptartas testavimo metodas buvo panaudotas atliekant sekančio skyriaus eksperimentą.

2.5. ES verifikavimas

Norint išsiaiškinti ES modelio tikslumą ir rezultatų pateikimo tikslumą bei aktualumą šių dienų saugos problemoms, buvo atliktas ES pateiktų rezultatų validacijos eksperimentas. Eksperimentui atlikti buvo pasitelkti magistrantūros informacinių technologijų ir informacijos saugos studijų kryptį studijuojantys studentai iš ITSfm-12 ir ITSfm-13 grupių. Studentai pasirinkti kaip ekspertai todėl, kad tokios studijų krypties studentai mokymo metu yra įgiję daug ir naujų žinių, susijusių su saugos problemomis, jų sprendimais ir taikomais metodais. Studentams leisti atlikti eksperimentą su sukurta ES buvo atsisakyta, kadangi norint gauti tikslesnius rezultatus, tektų papildomai ES pritaikyti eksperimentui, apribojant pateikiamus klausimus ir pasirenkamus vertinamų įmonių profilius. Eksperimentą atliekant su nepritaikyta sistema, išauga klaidų tikimybė dėl žmogiškojo faktoriaus. Todėl nuspręsta eksperimente dalyvaujantiems studentams pateikti klausimyną su identiškais klausimais ir leisti įvertinti saugos riziką pagal savo supratimą.

Eksperimento klausimynas yra sudarytas iš dviejų scenarijų, kuriuose nurodomas įmonės profilis, darbuotojų skaičius. Klausimynas sudarytas iš trisdešimties klausimų, po penkiolika kiekvienam scenarijui. Klausimai apima tokias grėsmes: IT įrangos, fizines, programinės įrangos, duomenų nutekinimo, žmonių sukeliamas ir trečių šalių teikiamų paslaugų. Abiejuose scenarijuose keturiolika klausimų yra vienodi, skiriasi tik faktai. Kiekvienas scenarijus turi po vieną klausimą, pritaikytą tiksliai pagal scenarijuje aprašytą įmonės profilį. Visi faktai, panaudoti kuriant klausimyną, buvo iš pradžių pateikti ekspertinei sistemai. Iš ES pateiktų rezultatų užpildytas atskaitinis ES klausimynas. Įsitikinta, jog ES rezultatai gauti tik remiantis klausimyne pateiktais faktais.

Ekspertai, pildydami klausimyną, nurodo tik tikimybės įvykti žalai vertes, kai galutinė rizikos vertė yra apskaičiuojama pagal antroje lentelėje pateiktą rizikos vertinimo matricą, kurią kaip vieną iš galimų vertinimo metodų siūlo ISO 27005 standartas [18]. Paprastesniam tikimybės įvykti tam tikram įvykiui ar žalai vertinimui, kiekviena vertybė yra pateikiama lentelėje, kurioje yra pateikiami papildomi vertinimui reikalingi faktai, tokie kaip: vertybės vertė ar svarba įmonės veiklai, taikomos saugos priemonės prieš tam tikras grėsmes, naudojama įranga, jos kiekis ar kaina ir kiti vertinimui svarbūs faktai.

Taip pat be tikimybės vertinimo studentai prie kiekvieno klausimo pateikė ir savo vertinimo priežastį, bei nurodė tikėtiną tikimybės mažinimo kaštų dydį. Svarbiausi eksperimentui naudotų scenarijų faktai pateikti trečioje lentelėje.

3 lentelė. Eksperimento scenarijai

	Scenarijus Nr.1	Scenarijus Nr.2
Įmonės profilis	Elektroninė komercija	Programavimo paslaugos
Darbuotojų skaičius	5	80
Stambios įrangos kiekis	20	10
Saugos politika	Ne	Taip

Iš viso eksperimente sudalyvavo devyni ekspertai. Bendrai iš eksperimento gautų rezultatų, galima teigti, jog ES pateikiami rezultatai, lyginant su realių ekspertų pateiktais rezultatais, yra tikrai patenkinami.

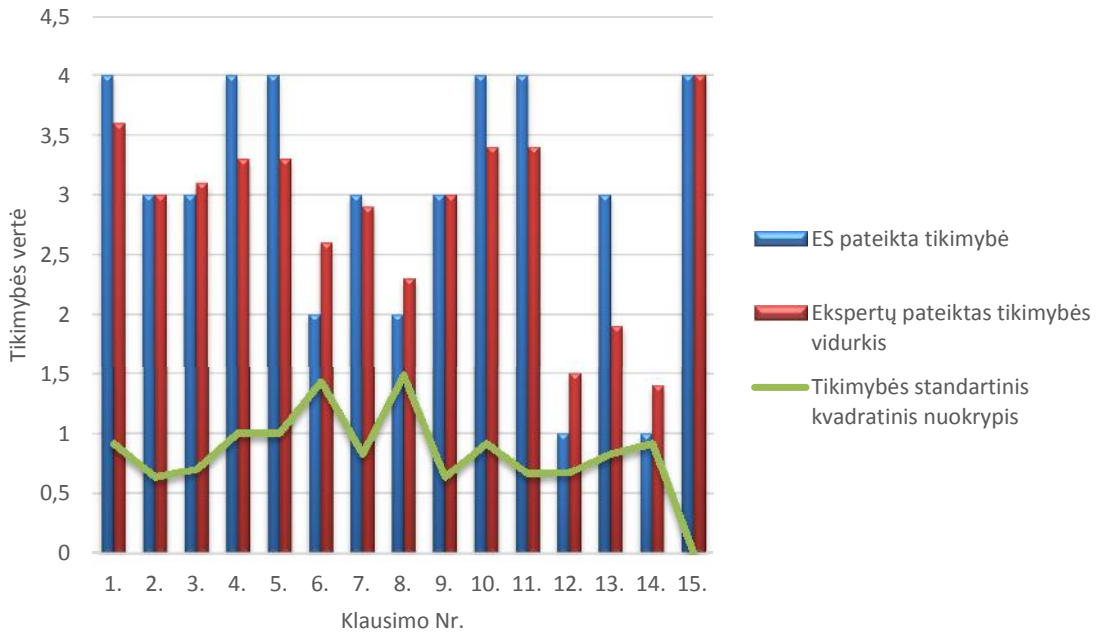
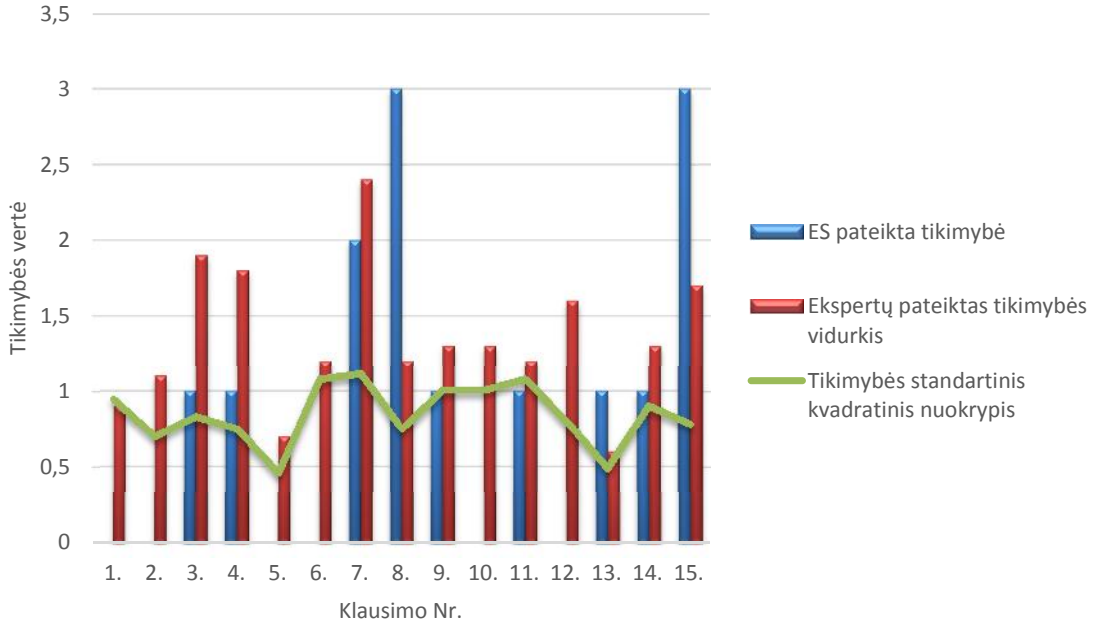
Atlikus eksperimentą visi duomenys yra susisteminti ir juos naudojant nubraižytos daugiausiai informacijos apie rezultatus teikiančios diagramos. Analizuoti eksperimento rezultatus panaudotos vidurkio, vidurkio nuokrypio, standartinio kvadratinio nuokrypio, imties centro ir pasikartojimo dažnumo statistinės analizės formulės. Toliau pateikiami ir smulkiau nagrinėjami eksperimento rezultatai pateikti diagramų pavidalu.

Žvelgiant į ketvirtoje lentelėje pateiktas diagramas matoma, jog ekspertų tikimybės vertinimas, palyginant su ES pateiktu vertinimu, yra labai panašus. Standartinis kvadratinis nuokrypis pirmame scenarijuje svyruoja nuo 0,6 iki 1,5, antrame nuo 0,5 iki 1. Pirmojo scenarijaus atveju, diagramoje matomos dvi standartinio kvadratinio nuokrypio didžiausias reikšmės, gautos dėl skirtingų nuomonių, vertinant stebėjimo ir saugos techninės įrangos reikalingumą mažoje įmonėje.

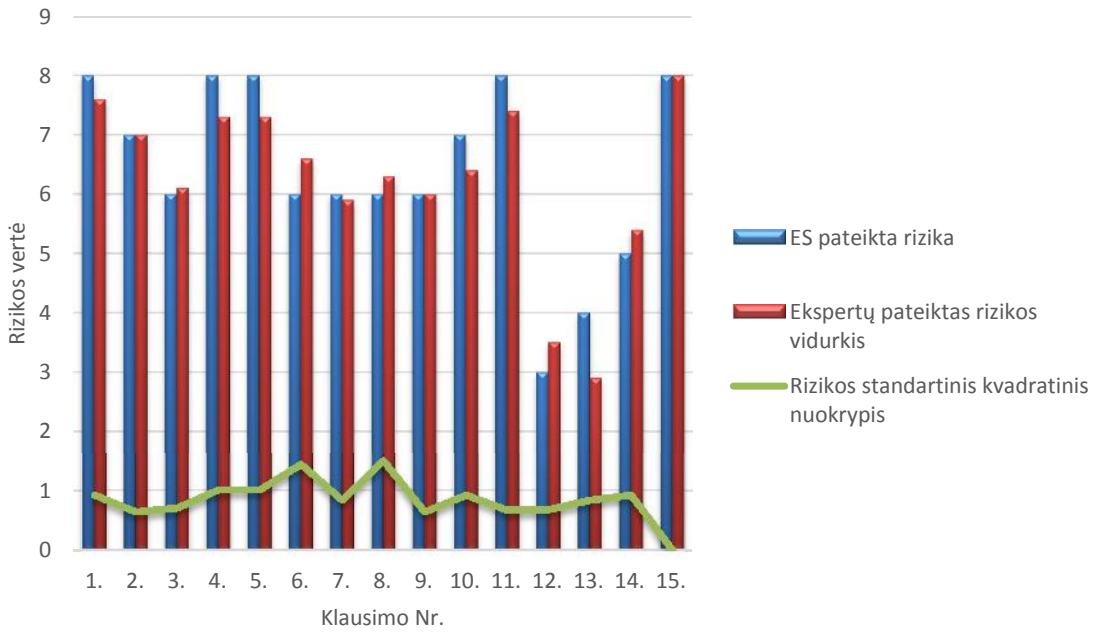
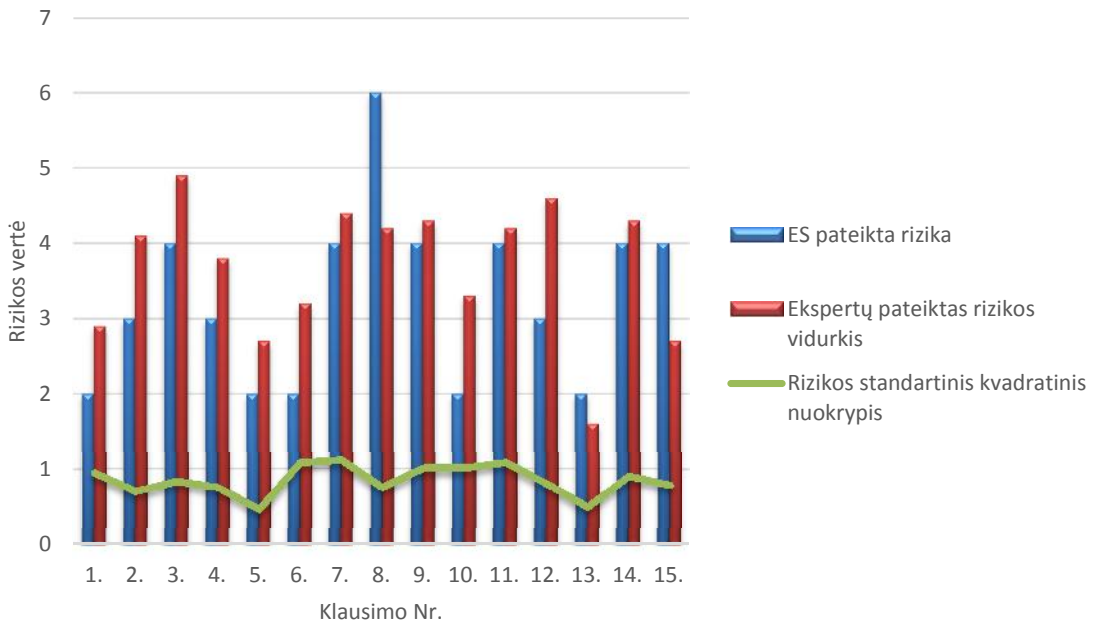
Analizuojant penktoje lentelėje pateiktas diagramas, galima dar kartą įsitikinti, jog ES rizikos vertinimas yra pakankamai tikslus, palyginant su ekspertų pateiktu vertinimu. Analizuojant tikimybės ir rizikos vertinimo diagramas kartu, galima pastebėti, jog vertinimo tikslumas priklauso nuo vertinimo verčių. Ribinių verčių klausimuose pastebimas mažesnis tikslumas, kadangi nustatyti riziką visiškai nesaugomai arba labai saugomai vertybei, reikalingi papildomi faktai arba smulkesnis rizikos vertinimas, kurie šiuo atveju pateikti nebuvo. Tai tuo pačiu patvirtina ir anksčiau minėtą faktą, jog ES sudarančių taisyklių skaičius yra proporcingas tiksliam rezultatui.

Tam tikras vertinimo tikslumas pastebėtas ir pagal klausimus bei pateiktas ekspertų vertinimo priežastis, kai techninė įranga ar priemonės, nesisiejančios su scenarijuje pateiktos įmonės profiliu, vertinamos skirtingai.

4 lentelė. ES ir ekspertų pateiktos tikimybės įvertinimo vertės

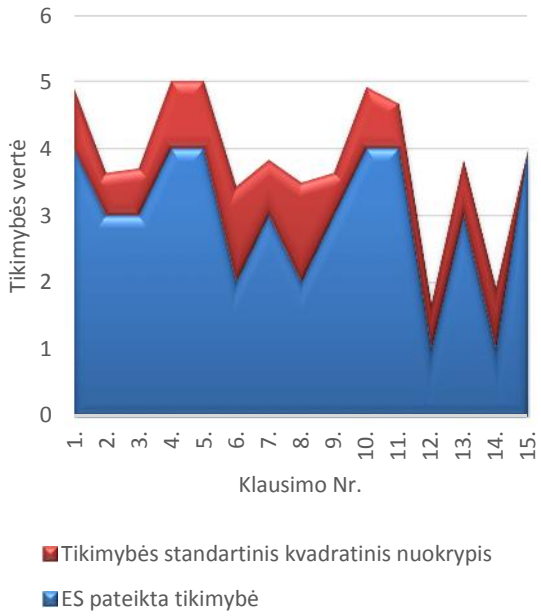
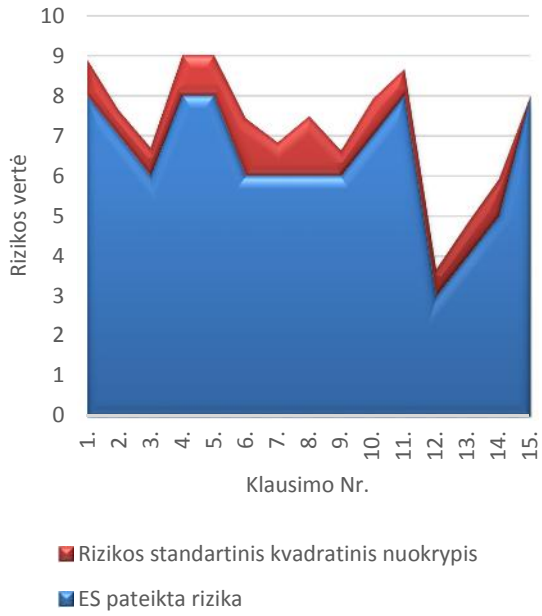
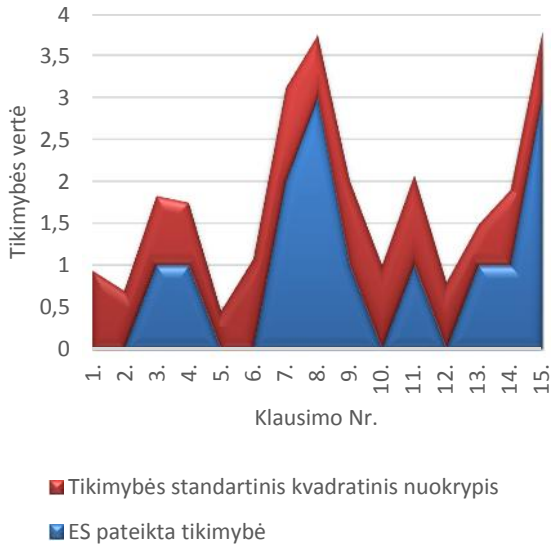
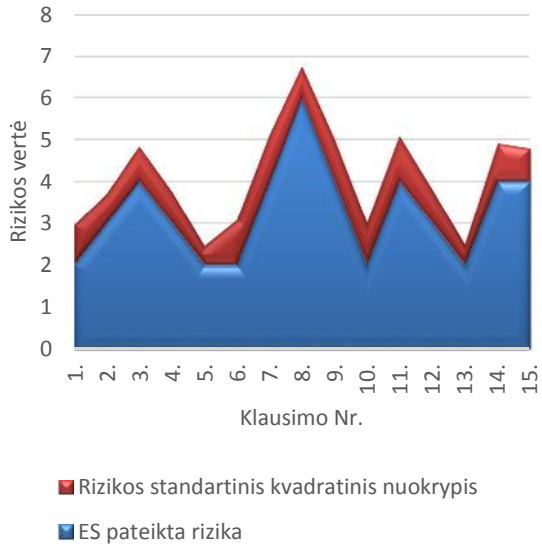
Nr.	Tikimybės verčių pasiskirstymas pagal klausimus
Scenarijus Nr.1	
Scenarijus Nr.2	

5 lentelė. ES ir ekspertų pateiktos rizikos įvertinimo vertės

	Rizikos verčių pasiskirstymas pagal klausimus
Scenarijus Nr.1	
Scenarijus Nr.2	

Iš šeštoje lentelėje pateiktų diagramų dar aiškiau matosi, jog didesni nuokrypiai atsiranda vertinant ribinėmis reikšmėmis. Abejuose scenarijuose pastebimas didesnis nuokrypis ties šeštu ir aštuntu klausimais. Tokius nuokrypius lėmė klausimų tipas ir pateikti tik du su klausimu tiesiogiai susiję faktai. Nors tai buvo klausimai, prie kurių buvo pateikta mažiausiai faktų, ES ir ekspertų vertinimo rezultatai yra patenkinami.

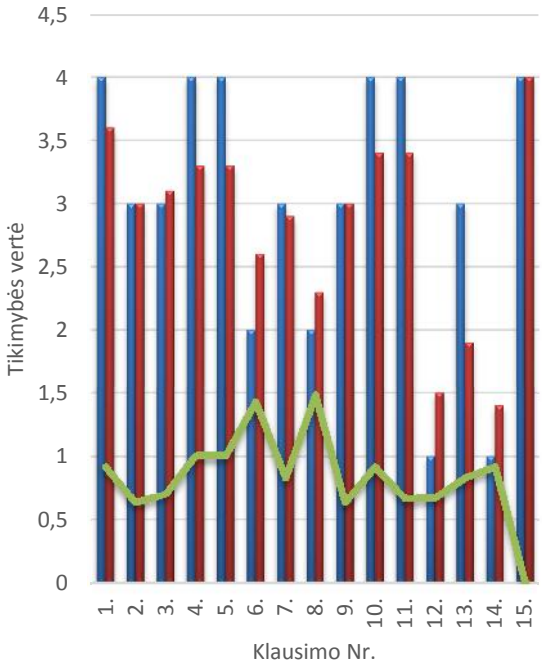
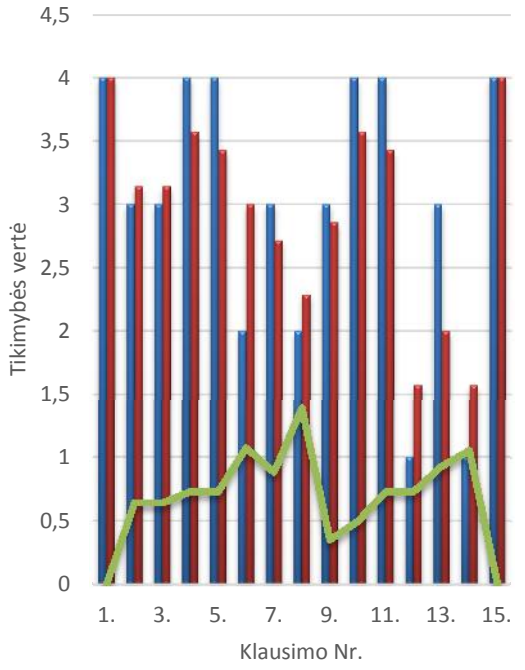
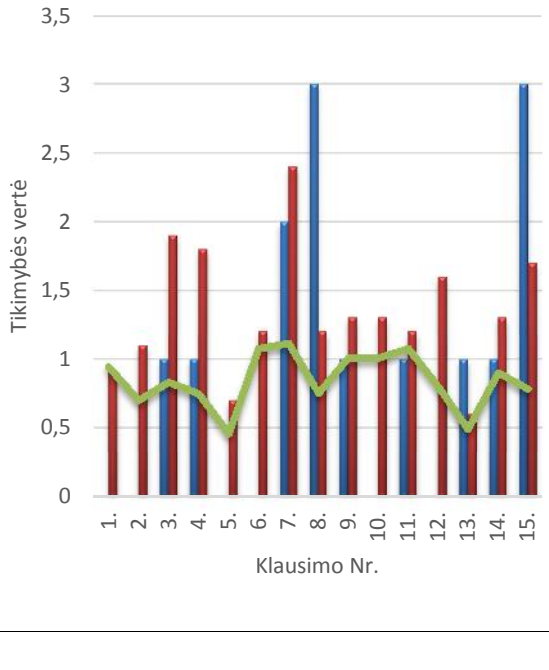
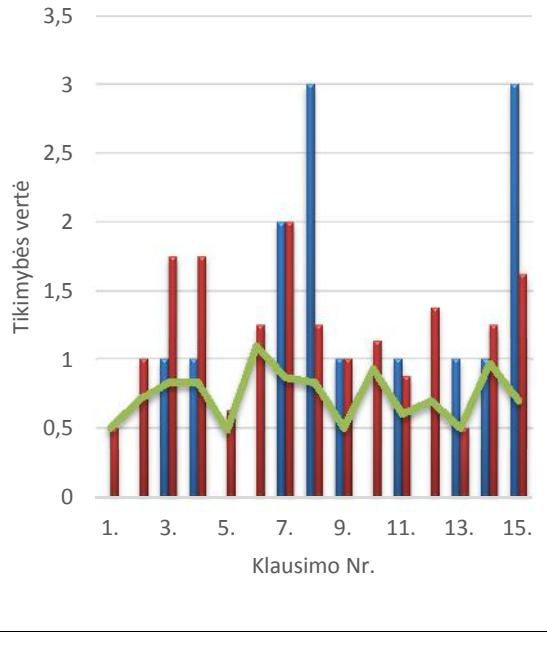
6 lentelė. ES ir ekspertų pateiktų tikimybės ir tikimybės nuokrypio vertinimo vertės

	Tikimybės nuokrypio pasiskirstymas pagal klausimus	Rizikos nuokrypio pasiskirstymas pagal klausimus
Scenarijus Nr.1		
Scenarijus Nr.2		

Išanalizavus įvairiais pjūviais gautus ekspertų anketavimo duomenis, yra pastebėta, jog dviejuose klausimynuose ekspertų atlikti vertinimai išsiskiria iš visų kitų (vertės neišsibarsčiusios, tikimybės vertinimo reikšmės vienodos, komentuojamos tikimybės įvertinimo priežastys netikslios arba jų išvis nėra). Atlikus gilesnę analizę, t.y. ištyrinėjus atsakymų pasikartojamumą, visiškai skirtingų situacijų įvertinimą tokia pačia tikimybės verte, apskaičiavus vidutines nuokrypio reikšmes ir tikimybės vidurkius pateiktų kaštų atžvilgiu, įsitikinta, jog pastebėtos anketos nėra objektyvios. Todėl buvo nuspręsta išbandyti pastebėtus netikslius klausimynus iš bendros statistikos panaikinti ir palyginti su prieš tai gautais rezultatais. Tokio bandymo rezultatai pateikti septintoje lentelėje. Pagal

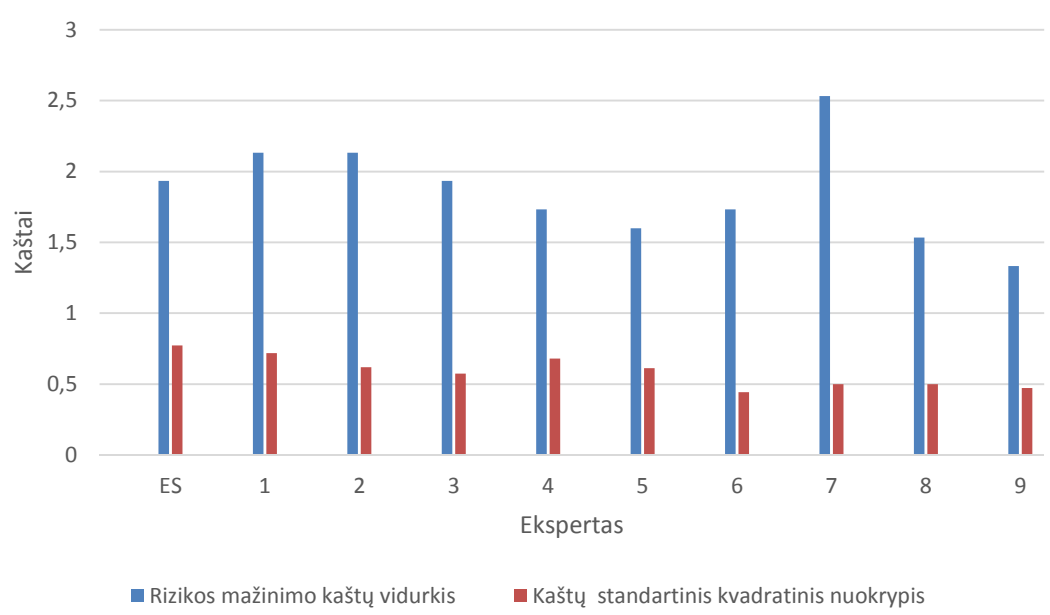
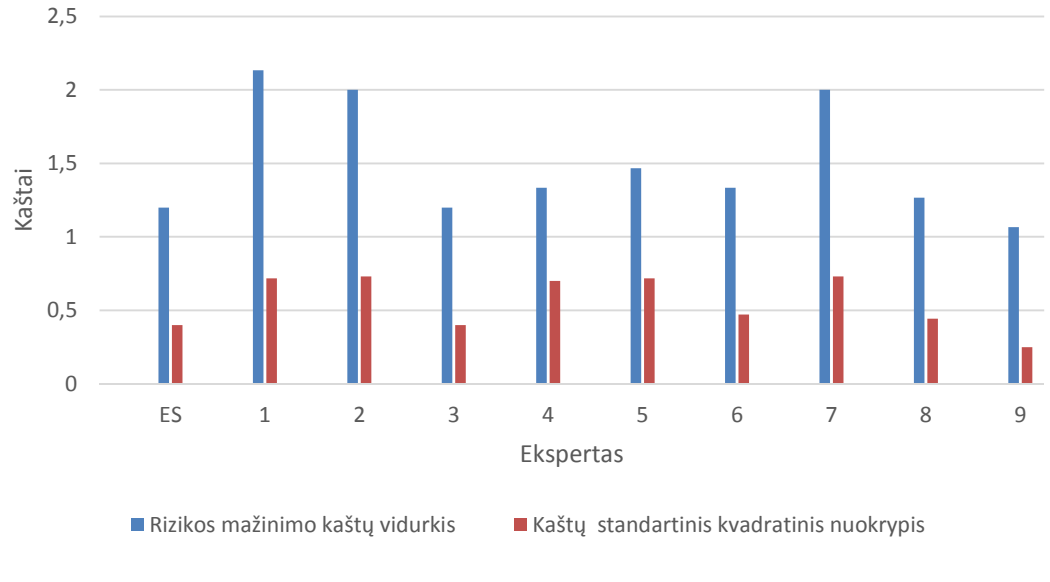
gautus rezultatus, akivaizdžiai ES ir ekspertų vertinimo tikslumas padidėjo, o standartinis kvadratinis nuokrypis sumažėjo.

7 lentelė. Eksperimento rezultatų duomenų tikrinimas

	Tikimybes vidurkio nuokrypio pasiskirstymas pagal visas anketas	Tikimybes vidurkio nuokrypio pasiskirstymas kai rezultatai gauti nenaudojant nekokybiškai užpildytų anketų
Scenarijus Nr.1		
Scenarijus Nr.2		

Iš ES ir ekspertų pateiktų rizikos mažinimo kaštų palyginimo gauti rezultatai rodo, kad pasirinktas trijų lygių kaštų vertinimo metodas yra per mažo tikslumo, kas matoma aštuntoje lentelėje pateiktose diagramose. Susiejus gautus rezultatus ir klausimus, pastebėta, jog kuo daugiau taikomų saugos priemonių, tuo sudėtingesnis rizikos mažinimo kaštų vertinimas. Rizikos mažinimo kaštų vertinimas trimis kainų lygiais buvo taikytas tik eksperimento metu, kadangi ES rizikos mažinimo kaštus pateikia penkiais kaštų lygiais, kaip ir rekomenduojama kaštus vertinti ISO 27005 standarte. Iš diagramų matyti, kad imant bet kurią eksperto pateiktą rizikos mažinimo kaštų vertę netikslumas galimas per vieną lygį.

8 lentelė. ES ir ekspertų rizikos mažinimo kaštų vertės

	Rizikos mažinimo kaštai pagal ekspertus
Scenarijus Nr.1	
Scenarijus Nr.2	

Apibendrintai iš gautų rezultatų ir įžvalgų galime spręsti, jog nustatant ribines tikimybės, turto vertės ar rizikos reikšmes, sistema turėtų naudoti daugiau faktų ar juos apimančių taisyklių tikslumui padidinti. Taip pat rizikos mažinimo kaštų rezultatų tikslumui reikia naudoti ne mažiau nei penkis kaštų lygius arba taikyti papildomus kaštų nustatymo metodus, kadangi iš eksperimento pastebėta, jog įvertinti tiksliai sunku net ekspertui, o dar sunkiau ES vartotojui.

Kuomet minimos sudėtingesnės rizikos įvertinimo galimybės dėl aukščiau išvardintų problemų, verta gerai apgalvoti rizikos analizės pradžioje pateikiamą pageidaujamą rizikos tolerancijos lygmens reikšmę. Jeigu rizikos analizė atliekama naudojant ekspertinę sistema, tai įvertinti yra labai paprasta, tereikia vieną kartą atlikus rizikos analizę, atlikti pakartotinę analizę, pasinaudojant jau pateiktais faktais iš XML rezultatų failo, nurodant kitą rizikos tolerancijos reikšmę. Tai yra, rizikos analizę galima atlikti, nurodant kelias toleruojamos rizikos reikšmes, taip atmetant galimybes tam tikrai rizikai dėl ribinės reikšmės būti nepastebėtai. Vertinant ekspertui, tokios tikslinančios ir pakartotino vertinimo galimybės yra ribotos laiko ir finansų prasme.

Išvados

1. Aptariamos ekspertinės sistemos yra naudojamos daugelyje sričių, bet ES, skirtos informacijos saugai valdyti, realiai egzistuoja tik integruotos į verslo valdymo sistemas arba yra labai siauros savo veikimo aprėptimi, taip negalėdamos užtikrinti viso informacijos saugos valdymo įmonėje.
2. Išnagrinėjus esamas ES kūrimo aplinkas, yra išsiaiškinta, jog šio ekspertinės sistemos modelio įgyvendinimui geriausiai tinka taisyklėmis pagrįsta ekspertinė sistema. Iš prieinamų ir atitinkančių iškeltus kriterijus ekspertinių sistemų yra pasirinkta JESS kūrimo aplinka. Išnagrinėjus JESS architektūrą ir jos komponentus, pateikti projektuojamai ES svarbiausi elementai ir jų Būlio logikos taikymo subtilybės, kas iš karto ir buvo pritaikyta, ir išbandyta, kuriant bandomąjį modelį.
3. Sukurta ekspertinė sistema veikia, taikant žinias trimis būdais: iš žinių bazės, dinaminės duomenų bazės, kurioje pateikti faktai gali būti aktualūs tuo laikotarpiu, arba iš abiejų bazių vienu metu. Galimybė taikyti istorines žinias papildo ekspertinę sistemą DSS funkcionalumu. Tokiu būdu ES gali pateikti tikslesnius rezultatus arba, norint aprašyti tam tikrą vertybę ir galimas grėsmes, tai padaryti leidžia su mažesniu taisyklių kiekiu.
4. Atlikus eksperimentą, buvo patvirtinta ES pritaikymo galimybė informacijos saugos sričiai. ES pateikiami rezultatai, palyginant su ekspertų rezultatais, yra pakankamai tikslūs, atkreipiant dėmesį į palyginti mažą faktų ir taisyklių kiekį pateiktoje ES. Detaliai išanalizavus eksperimento rezultatus ir diagramas, galima patvirtinti tokius ES privalumus, palyginant su žmonėmis ekspertais, kaip ne emocingumas, pastovumas, didelis greitis ir žinios iš daugelio ekspertų. ES gali būti ne tik lygiavertė, vertinant riziką gyvo eksperto atžvilgiu, o panaudojus dinaminę rizikos analizės faktų bazę, kurioje būtų talpinami rizikos analizę atliekamu laikotarpiu tikslinti padedantys kriterijai ir faktai, net ir tikslesnė nei žmogus ekspertas.
5. Eksperimento metu pastebėta, jog, atliekant ribinės vertės rizikos vertinimą iš vidutinio kiekio taisyklių, mažėja vertinimo tikslumas ne tik ekspertinės sistemos atžvilgiu bet ir ekspertų. Ekspertinės sistemos atžvilgiu didinti tikslumą galima, keičiant rizikos tolerancijos lygį arba panaudojant papildomas taisykles, kai žmogaus eksperto atveju, kai kuriuos rizikos vertinimo etapus reikia atlikti iš naujo. Papildomas ES privalumas yra tas, kad keičiant rizikos tolerancijos reikšmę, ES sistemos pateiktuose rezultatuose yra galimybė identifikuoti netikslumus, kas žmogaus eksperto atveju yra sudėtinga.

6. Darbe pateiktame ES modelyje paaiškėjo ir trūkumai, susiję su ES sistemos kūrimo aplinkos naudojimu, kurių iš teorinės medžiagos pastebėta nebuvo. Tai skirtinga darna tarp JESS aplinkos versijų, taisyklių vizualizavimo dėl neatnaujinamų įskiepių negalimumas, mažesnis nei tikėtasi funkcionalumas, kai nevartojama JAVA kalba.

Literatūra

[1] Amin-Naseri, M. R.; Neshat, N. 2011. An Expert System Based on Analytical Hierarchy Process for Diabetes Risk Assessment (DIABRA), in *Advances in Swarm Intelligence*. Vol. 6729. Springer Berlin Heidelberg. 252-259.

[2] Angeli, C. 2000. An online expert system for fault diagnosis in hydraulic systems, in *13th International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems.* Springer-Verlag New York. 184-191.

[3] Bennett, S. P.; Kailay, M. P. 1992. An application of qualitative risk analysis to computer security for the commercial sector, in *Eight Annual IEEE Computer Security Applications Conference*. IEEE Computer Society Press. New York. 64-73.

[4] Blackley, J. A.; Peltier, T. R. 2005, *Information Security Risk Analysis*. United States of America: CRC Press.

[5] Bodine, L. Delivering legal services via Web-based expert systems: Law firms find new paths to profit on the Web. [Online]. 2001. [cited 15 September 2013]. Available from internet <http://www.sugarcrest.com/newsletters/ v1_issue4.htm>.

[6] Cernik, J. 2009. Framework For An Expert System Generator: A thesis, Master of science.

[7] Cowell, R. G.; Dawid, P.; Lauritzen, S. L.; Spiegelhalter, D. J. 2007, *Probabilistic Networks and Expert Systems: Exact Computational Methods for Bayesian Networks*. Springer.

[8] Dym, C. L. 1985. EXPERT SYSTEMS: New Approaches to Computer-aided Engineering, in *Engineering with Computers.* Vol. 1. No. 1. Springer-Verlag, 9-25.

[9] Dymova, L.; Sevastianov, P.; Bartosiewicz L. 2010. A new approach to the rule-base evidential reasoning: Stock trading expert system application, in *Expert Systems with Applications*. Volume 37. Issue 8. Tarrytown, NY, USA: Pergamon Press. 5564-5576.

[10] Durkin, J. 1994, *Expert Systems: Design and Development*. New York: Macmillan.

[11] Eberlein, A.; Crowther, M.; Halsall, F. 1997. Development of new telecommunications services using an expert system, in *BT Technology Journal.* Vol. 15. No. 1. Kluwer Academic Publishers. 217-222.

[12] Friedman-Hill, E. 2003, *Jess in Action. Rule-Based Systems in Java*. Greenwich: Manning Publications Co.

[13] Giarratano, J. C.; Riley, G.D. 1998, Giarratano, *Expert Systems: Principles and Programming.* 3rd ed. United States of America: Course Technology.

[14] Goztepe, K. 2012. Designing a Fuzzy Rule Based Expert System for Cyber Security, in *INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE. V*ol. 1. No. 1. 13-19.

[15] Grosan, C.; Abraham, A. 2011, *Intelligent Systems. A Modern Approach*. Berlin: Springer.

[16] Gwo-Jen Hwang, Chieh-Yuan Chen, Pei-Shan Tsai, Chin-Chung Tsai. 2011. An expert system for improving web-based problem-solving ability of students, in *Expert Systems with Applications*. Vol. 38. Tarrytown, NY, USA: Pergamon Press. 8664-8672.

[17] *International Standard ISO/IEC 27001. Information technology - Security techniques - Information security management systems – Requirements. ISo/IEC 27001:2005(SE).* Geneve. 2005. 34 p.

[18] *International Standard ISO/IEC 27005. Information technology - Security techniques - Information security risk management. BS ISO/IEC 27005:2008.* London. 2008. 55 p.

[19] Inventory of Risk Management - Risk Assessment methods and tools. Smart Information Security Management System (SISMS). [Interaktyvus]. ENISA. [žiūrėta 2013-01-04]. Prieiga per internetą: <http://rm-inv.enisa.europa.eu/tools/t_sisms.html>.

[20] Kailay, M. P.; Jarratt, P. 1995. RAMeX: a prototype expert system for computer security risk analysis and management, in *Computers & Security-COMPSEC.* Vol. 14. Elsevier Science. 449-463.

[21] Kozhakhmet, K.; Bortsova, G.; Inoue, A.; Atymtayeva, L. Expert System for Security Audit Using Fuzzy Logic. in *Proceedings of the 23rd Midwest Artificial Intelligence and Cognitive Science Conference (MAICS2012).* Cincinnati, OH. 146-151.

[22] Krishnamoorthy, C.S.; Rajeev, S. 1996, *Artificial Intelligence and Expert Systems for Engineers*. United States: CRC Press.

[23] Kulvietis, G.; Kulvietienė, R.; Rudzkienė, V. 1996, *Įvadas į dirbtinio intelekto ir ekspertinių sistemų kursą*. Vilnius: Technika.

[24] Leon, C.; Biscarri, F.; Monedero, I.; Guerrero, I. J.; Biscarri, J.; Millan, R. 2011. Integrated expert system applied to the analysis of non-technical losses in power utilities, in *Expert Systems with Applications*. Volume 38. Issue. 38. Elsevier Science. 10247-10285.

[25] Lindqvist, U.; Porras, P. A. 1999. Detecting Computer and Network Misuse Through the Production-Based Expert System Toolset (P-BEST), in *In Proceedings of the 1999 IEEE Symposium on Security and Privacy.* Oakland, CA. 9-12.

[26] Lucas, P. 2006. Expert Systems, in *Encyclopedia of Life Support Systems of UNESCO*.

[27] McCullough, D.; Rambow, O.; Barzilayy, R. 1998. A New Approach To Expert System Explanations, in *9th International Workshop on Natural Language Generation.* Niagara-on-the-lake. Ontario. Canada. 78-87.

[28] Negnevitsky, M. 2005, *Artificial Intelligence - A Guide to Intelligent Systems*. 2nd Edition. Harlow, England: Pearson Education.

[29] Nikolopoulos, C. 1997, *Expert Systems: Introduction to First and Second Generation and Hybrid Knowledge Based Systems*. New York: CRC Press.

[30] O'Brien, L.; Cai, R.; Zhang, H.; Li, Z. 2012. Building an Expert System for Evaluation of Commercial Cloud Services, in *CSC '12 Proceedings of the 2012 International Conference on Cloud and Service Computing*. IEEE Computer Society Washington. 168-175.

[31] Pourdarab, S.; Nadali, A.; Nosratabadi, H. E. 2011. Risk Assessment of Information Technology Projects Using Fuzzy Expert System, in *Digital Information*

and Communication Technology and Its Applications. Vol. 166. Springer Berlin Heidelberg. 563-576.

[32] Ritendra, G. 2008, *E-commerce*. New Delhi: New Age International Pvt Ltd Publishers.

[33] Romana, S.; Phadnis, S.; Pareek, H.; Eswari, P. R. L. 2011. Behavioral Malware Detection Expert System – Tarantula, in *Advances in Network Security and Applications.* Vol. 196. Springer Berlin Heidelberg. 65-77.

[34] Ross, T. J. 2010, *Fuzzy logic with engineering applications*. 3rd Edition. Chennai, India: John Wiley & Sons.

[35] Ruiz-Mezcua, B.; Garcia-Crespo, A.; Lopez-Cuadrado, J. L. 2011. An expert system development tool for non AI experts, in *Expert Systems with Applications: An International Journal. V*ol. 38. Tarrytown, NY, USA: Pergamon Press, 597-609.

[36] Sajja, P. S.; Akerkar, R. 2010, *Knowledge-Based Systems*. United States of America: Jones & Bartlett.

[37] Sauter, V. L. 2010, *Decision Support Systems For Business Intellgence.* 2nd Edition. New Jersey: John Wiley & Sons.

[38] Schalkoff, R.J. 2011, *Intelligent Systems: Principles, Paradigms and Pragmatics*. United States of America: Jones & Bartlett Publishers.

[39] Schank, R.C.; Childers, P. G. 1984, *The Cognitive Computer: on Language, Learning and Artificial Intelligence*. New York: Pearson Addison-Wesley.

[40] Selvani Deepthi, K.; Srinivasa Rao, D.; Naresh Kumar, T.; Sugunakar Naidu, L. 2011. Troubleshooting Wireless Mesh Networks using Rule-Based Expert System, in *IJECT*. Vol. 2. No. 2. 22-25.

[41] Siler, W. ; Buckley, J. J. 2005, *Fuzzy Expert Systems and Fuzzy Reasoning.* 1st ed. United States of America: Wiley.

[42] Summers, R.; Tsudik, G. 1991. AudES - an Expert System for Security Auditing, in *In Proceedings of the AAAI Conference on Innovative Application in Artificial Intelligence*. AAAI Press. 221-232.

[43] Tocatlidou, A.; Passam, H. C.; Sideridis, A. B.; Yialouris, C. P. 2002. Reasoning under uncertainty for plant disease diagnosis, in *Expert Systems*. Vol. 19. 46-52.

[44] Zargham, M. R.; Mogharreban, N. 2005. PORSEL: an expert system for assisting in investment analysis and valuation, in *Soft Computing*. Volume 9. Issue 10. Springer-Verlag. 742-748.

Priedai

1 priedas

Pavyzdiniai ekspertinės sistemos pateikiami klausimai

#Koks įmonės veiklos profilis? Įveskite profilio numerį iš pateikto sąrašo: 1.E-komercija 2.Programavimas 3.Dizainas 4.Transportas 5.Medicinos kabinetas

#Kiek įmonėje yra darbuotojų? (1-250)

#Ar įmonės patalpos yra nuomojamos?

#Ar patalpos yra nuomojamos kartu su įmonės veiklai reikalingomis priemonėmis? (Pvz., verslo inkubatorius)

#Ar naudojama įranga yra nuomojama?

#Ar visa įmonės įranga ir infrastruktūra yra prižiūrima trečios šalies?

#Ar įmonės teritorija saugoma?

#Ar įmonėje yra saugos specialistas/-ų? Kiek? (0 - Specialisto nėra, jeigu yra, nurodykite specialistų skaičių)

#Ar įmonė savo IT ūkį prižiūri pati?

#Ar įmonė savo visą infrastruktūrą prižiūri pati?

#Ar įmonėje yra interneto ryšys?

#Įvertinkite interneto ryšio svarbumą įmonės veiklai? (Nuo 0 iki 4. Didesnis skaičius reiškia didesnę svarbą įmonei)

#Ar interneto ryšys yra laidinis?

#Ar įmonė yra netoli vandens telkinių, kuriuose vandens lygis gali pakilti?

#Ar aplink įmonės teritoriją yra didesnei gaisro rizikai priskirtų statinių?

#Ar įmonė vykdo sistemų stebėseną?

#Ar įmonė vykdo visų sistemų stebėseną (patalpų, sistemų, tinklų)?

#Ar įmonėje vyksta mokymai saugos tema?

#Ar įmonėje yra vykdoma turto saugos politika?

#Ar įmonės turto fizinės saugos lygis didesnis nei vidutinis?

#Ar įmonės turto saugos politikoje išskirta informacijos sauga?

#Ar įmonėje vykdomi kokie nors/bet kokie metiniai reagavimo planai?

#Ar įmonė planuoja sistemos techninius ir programinius resursus bent pusmečiui į priekį?

#Įvertinkite dešimtbalėje sistemoje įsivaizduojamą įmonės atsparumą saugos incidentams?

#Ar įmonė yra kada nors turėjusi saugos incidentų?

#Ar įmonėje vyksta informacijos mainai, tiesioginė prieiga prie įmonės informacijos?

#Ar įmonėje yra laikomas minimalus kiekis perteklinės įrangos incidentams?

#Ar įmonėje atlikta rizikos analizė?

#Ar įmonėje yra patvirtinta ir taikoma saugos politika?

#Ar įmonė taiko standartizuotą saugos politiką?

#Ar įmonė vykdo visus standarto reikalavimus be išimčių?

#Ar įmonė taiko dalinius standarto punktus?

#Ar įmonėje yra vykdoma saugos politika darbuotojų atžvilgiu juos įdarbinant/dirbant/atleidžiant?

#Ar įmonė turi tiesioginį priėjimą prie klientų apmokėjimo priemonių duomenų?

#Ar įmonėje saugomi klientų apmokėjimo duomenys yra šifruoti vienpusiu šifravimo algoritmu?

#Ar įmonėje yra vykdoma periodinė informacijos saugos patikra?

#Ar įmonėje vartotojų duomenys prilyginami kritiniams įmonės duomenims?

#Ar įmonėje skirtingi procesai yra izoliuoti vienas nuo kito?

#Ar įmonės komunikacijos yra segmentuotos ir aprašytos jų procedūros?

#Ar įmonėje bendravimo su klientais kanalais siunčiama informacija yra tikrinama?

#Ar įmonė turi 24/7 svarbiausių veiklos procesų stebėsenos sistemą?

#Ar reagavimas į stebėsenos sistemos pranešimus yra 24/7?

#Ar įmonės surinkti statistiniai duomenys integruojami į tolesnius įmonės veiklos procesus?

#Ar įmonė taiko kokias nors saugaus programavimo gerąsias praktikas?

#Ar įmonėje kuriamų produktų kūrimo/testavimo/produkcijos duomenų-talpyklos/tinklas segmentuotas?

#Ar yra asmenų, galinčių prieiti prie nebaigtų/baigtų produktų ir juos nukopijuoti nepaliekant pėdsakų?

#Ar pateikiant pavyzdinius, reklaminius produktus klientui išeities kodas būna obfuskuotas/šifruotas?

#Ar įmonė stebi informacijos srautus, susijusius su darbuose naudojamomis programavimo kalbomis?

#Ar įmonėje taikoma suminio šifravimo technologija?

#Ar klientų ir darbuotojų bendravimas elektroniniais kanalais paraleliai pateikiamas vadovaujantiems asmenims?

#Ar įmonėje naudojami vandens ženklai iki darbas yra atiduodamas klientui?

#Ar įmonės demonstracinių/reklaminių darbų pateikimas yra apsaugotas?

#Ar naudojamų bevielių įrenginių šifravimo mechanizmai atitinka minimalius šiuolaikinius reikalavimus? (Planšetės, projektoriai)

#Ar įmonėje atsižvelgiama į skirtingų platformų įrenginių suderinimą saugumo požiūriu?

#Ar įmonės transportas turi nuotolinio sekimo/registravimo įrangą?

#Ar registravimo/sekimo įrangos sukauptiems duomenims taikomas prailginto saugojimo laikotarpis?

#Ar įmonė naudoja elektroninę transporto valdymo sistemą?

#Ar klientų duomenų bazei taikomos papildomo saugumo priemonės?

#Ar įmonės turi atskirą žurnalą, patirtų įvykių registravimui?

#Ar įmonėje naudojamiems atsiskaitymams prioritetas teikiamas elektroniniam būdui?

#Ar skiriamas papildomas saugumas finansiniams ir atskaitos dokumentams?

#Ar įmonėje tachogramos priskirtos konfidencialiai įmonės informacijai?

#Ar įmonė talpina duomenis apie pacientus savo duomenų bazėje?

#Ar įmonėje esantys duomenų mainai registruojami žurnaluose?

#Ar įmonėje laikinai yra saugoma spausdintuvais, kopijuokliais atliktų darbų kopijos?

#Ar kritinių įrenginių naudojimas galimas tik po autentifikacijos?

#Ar įmonėje uždraustos visų tipų išorinės duomenų laikmenos?

#Ar visa informacija, kuri būna registruojama popieriniuose žurnaluose dubliuojama elektroniniuose?

#Ar yra taikomos saugumo priemonės prieš sukčiavimą (phishing)?

#Ar yra taikomos saugumo priemonės aparatinės įrangos gedimų rizikai mažinti?

#Ar yra taikomos saugumo priemonės elektros maitinimo praradimo rizikai mažinti?

#Ar yra taikomos saugumo priemonės DDoS rizikai mažinti?

#Ar yra taikomos saugumo priemonės gaisro rizikai mažinti?

#Ar yra taikomos saugumo priemonės užliejimo rizikai mažinti?

#Ar yra taikomos saugumo priemonės pilno sistemos resursų išnaudojimo (sistemos persipildymo) rizikai mažinti?

#Ar yra taikomos saugumo priemonės programinės įrangos veiklos sutrikimų rizikai mažinti?

#Ar yra taikomos saugumo priemonės nesankcionuotai duomenų ar programinės įrangos kopijavimo rizikai mažinti?

#Ar yra taikomos saugumo priemonės informacijos pakeitimo arba sunaikinimo rizikai mažinti?

#Ar yra taikomos saugumo priemonės piratinės programinės įrangos naudojimo rizikai mažinti?

#Ar yra taikomos saugumo priemonės virusų ir kenksmingo programinio kodo rizikai mažinti?

#Ar yra taikomos saugumo priemonės galimam darbuotojų nesilaikymui saugumo reikalavimų rizikai mažinti?

#Ar yra taikomos saugumo priemonės galimai laikmenų arba dokumentų vagystės rizikai mažinti?

#Ar yra taikomos saugumo priemonės slaptažodžių atskleidimui?

#Ar yra taikomos saugumo priemonės informacinės sistemos priežiūros spragų rizikai mažinti?

#Ar yra taikomos saugumo priemonės nesankcionuotai aparatinės įrangos keitimo rizikai mažinti?

#Ar yra taikomos saugumo priemonės įsibrovimo iš interneto rizikai mažinti?

#Ar yra taikomos specialios saugumo sutartys su išorinėmis šalimis?

#Ar įmonėje aprašyta turto valdymo politika?

#Ar įmonėje visas turtas inventorizuotas?

#Ar kiekvienas turto vienetas turi savo priskirtą naudotoją?

#Ar yra taikomos turto valdymo/naudojimo/saugojimo taisyklės?

#Ar įmonėje vykdoma informacijos klasifikacija?

#Ar įmonėje informacijai klasifikuoti taikomos politikos gairės?

#Ar informacijos klasifikacija ir jos tvarkymas apibrėžtas procedūromis?

Pavyzdinės ekspertinės sistemos taisyklės

```
(defrule assert-kpk-pirat-risk-11
(answer (ident irang_komp) (text taip))
(answer (ident irang_komp_v) (text ?d&:(= ?d 1)))
(answer (ident risk_mit_soft_pirat) (text ne))
(answer (ident risk_mit_kpk) (text ne))
(answer (ident risk_mit_soft) (text ne))
 =>
(assert (answer (ident kpk-pirat_risk) (text 2)))
(assert (answer (ident kpk-pirat_risk_mitigation) (text "maži")))
(assert (answer (ident kpk-pirat_risk_reason) (text "kompiuterių programinės įrangos gedimai įmonei mažai svarbūs ir jai netaikomos apsaugos priemonės. Privaloma taikyti saugumo priemones programinės įrangos veiklos sutrikimų rizikai mažinti. Rekomenduojama taikyti KPK ir/arba piratinės programinės įrangos apsaugos priemones"))))

(defrule assert-kpk-pirat-risk-12
(answer (ident irang_komp) (text taip))
(answer (ident irang_komp_v) (text ?d&:(= ?d 2)))
(answer (ident risk_mit_soft_pirat) (text ne))
(answer (ident risk_mit_kpk) (text ne))
(answer (ident risk_mit_soft) (text ne))
 =>
(assert (answer (ident kpk-pirat_risk) (text 4)))
(assert (answer (ident kpk-pirat_risk_mitigation) (text "maži")))
(assert (answer (ident kpk-pirat_risk_reason) (text "kompiuterių programinės įrangos gedimai įmonei vidutiniškai svarbūs ir jai netaikomos apsaugos priemonės. Privaloma taikyti saugumo priemones programinės įrangos veiklos sutrikimų rizikai mažinti. Taip pat reikalinga taikyti KPK ir/arba piratinės programinės įrangos apsaugos priemones"))))

(defrule assert-kpk-pirat-risk-13
(answer (ident irang_komp) (text taip))
(answer (ident irang_komp_v) (text ?d&:(= ?d 3)))
(answer (ident risk_mit_soft_pirat) (text ne))
(answer (ident risk_mit_kpk) (text ne))
(answer (ident risk_mit_soft) (text ne))
 =>
(assert (answer (ident kpk-pirat_risk) (text 6)))
```

```
      (assert    (answer    (ident    kpk-pirat_risk_mitigation)    (text
"vidutiniai")))

      (assert (answer (ident kpk-pirat_risk_reason) (text "kompiuterių
programinės įrangos gedimai įmonei svarbūs ir jai netaikomos apsaugos
priemonės. Privaloma taikyti saugumo priemones programinės įrangos veiklos
sutrikimų rizikai mažinti, taikyti KPK ir/arba piratinės programinės įrangos
apsaugos priemones"))))


      (defrule assert-kpk-pirat-risk-14

      (answer (ident irang_komp) (text taip))

      (answer (ident irang_komp_v) (text ?d&:(= ?d 4)))

      (answer (ident risk_mit_soft_pirat) (text ne))

      (answer (ident risk_mit_kpk) (text ne))

      (answer (ident risk_mit_soft) (text ne))

       =>

      (assert (answer (ident kpk-pirat_risk) (text 7)))

      (assert (answer (ident kpk-pirat_risk_mitigation) (text "dideli")))

      (assert (answer (ident kpk-pirat_risk_reason) (text "kompiuterių
programinės įrangos gedimai įmonei yra kritiniai, o jai apsaugoti visiškai
netaikomos apsaugos priemonės. Privaloma taikyti saugumo priemones
programinės įrangos veiklos sutrikimų rizikai mažinti, KPK ir piratinės
programinės įrangos apsaugos priemones, stebėseną."))))


      (defrule assert-kpk-pirat-risk-21

      (answer (ident irang_komp) (text taip))

      (answer (ident irang_komp_v) (text ?d&:(= ?d 2)))

      (answer (ident risk_mit_soft_pirat) (text taip))

      (answer (ident risk_mit_kpk) (text ne))

      (answer (ident risk_mit_soft) (text ne))

       =>

      (assert (answer (ident kpk-pirat_risk) (text 3)))

      (assert (answer (ident kpk-pirat_risk_mitigation) (text "maži")))

      (assert (answer (ident kpk-pirat_risk_reason) (text "kompiuterių
programinės įrangos gedimai įmonei vidutiniškai svarbūs. Gedimų vengimui
naudojama tik piratinės programinės įrangos apsaugos priemonės. Rizikai
mažinti rekomenduojama taikyti KPK ir/arba programinės įrangos veiklos
sutrikimų apsaugos priemones."))))


      (defrule assert-kpk-pirat-risk-22

      (answer (ident irang_komp) (text taip))

      (answer (ident irang_komp_v) (text ?d&:(= ?d 2)))

      (answer (ident risk_mit_soft_pirat) (text taip))

      (answer (ident risk_mit_kpk) (text taip))
```

```
(answer (ident risk_mit_soft) (text ne))
 =>
(assert (answer (ident kpk-pirat_risk) (text 2)))
(assert (answer (ident kpk-pirat_risk_mitigation) (text "labai maži")))
(assert (answer (ident kpk-pirat_risk_reason) (text "kompiuterių programinės įrangos gedimai įmonei vidutiniškai svarbūs. Gedimų vengimui naudojama piratinės programinės įrangos ir KPK apsaugos priemonės. Rizikai mažinti rekomenduojama taikyti programinės įrangos veiklos sutrikimų saugumo priemones."))))

(defrule assert-kpk-pirat-risk-23
(answer (ident irang_komp) (text taip))
(answer (ident irang_komp_v) (text ?d&:(= ?d 2)))
(answer (ident risk_mit_soft_pirat) (text taip))
(answer (ident risk_mit_kpk) (text ne))
(answer (ident risk_mit_soft) (text taip))
 =>
(assert (answer (ident kpk-pirat_risk) (text 3)))
(assert (answer (ident kpk-pirat_risk_mitigation) (text "maži")))
(assert (answer (ident kpk-pirat_risk_reason) (text "kompiuterių programinės įrangos gedimai įmonei vidutiniškai svarbūs. Gedimų vengimui naudojama piratinės programinės įrangos ir veiklos sutrikimų saugumo priemones. Rizikai mažinti rekomenduojama taikyti ir KPK apsaugos priemonės."))))

(defrule assert-kpk-pirat-risk-24
(answer (ident irang_komp) (text taip))
(answer (ident irang_komp_v) (text ?d&:(= ?d 2)))
(answer (ident risk_mit_soft_pirat) (text taip))
(answer (ident risk_mit_kpk) (text taip))
(answer (ident risk_mit_soft) (text taip))
 =>
(assert (answer (ident kpk-pirat_risk) (text 2)))
(assert (answer (ident kpk-pirat_risk_mitigation) (text "maži")))
(assert (answer (ident kpk-pirat_risk_reason) (text "kompiuterių programinės įrangos gedimai įmonei vidutiniškai svarbūs. Gedimų vengimui naudojama piratinės programinės įrangos, KPK ir programinės įrangos veiklos sutrikimų apsaugos priemonės. Rizikai mažinti rekomenduojama taikyti papildomas stebėsenos priemones."))))

(defrule assert-kpk-pirat-risk-31
(answer (ident irang_komp) (text taip))
```

```
(answer (ident irang_komp_v) (text ?d&:(= ?d 3)))
(answer (ident risk_mit_soft_pirat) (text taip))
(answer (ident risk_mit_kpk) (text ne))
(answer (ident risk_mit_soft) (text ne))
 =>
(assert (answer (ident kpk-pirat_risk) (text 4)))
(assert (answer (ident kpk-pirat_risk_mitigation) (text "maži")))
(assert (answer (ident kpk-pirat_risk_reason) (text "kompiuterių programinės įrangos gedimai įmonei svarbūs. Gedimų vengimui naudojama tik piratinės programinės įrangos apsaugos priemonės. Rizikai mažinti rekomenduojama taikyti KPK ir/arba programinės įrangos veiklos sutrikimų apsaugos priemones."))))

(defrule assert-kpk-pirat-risk-32
(answer (ident irang_komp) (text taip))
(answer (ident irang_komp_v) (text ?d&:(= ?d 3)))
(answer (ident risk_mit_soft_pirat) (text taip))
(answer (ident risk_mit_kpk) (text taip))
(answer (ident risk_mit_soft) (text ne))
 =>
(assert (answer (ident kpk-pirat_risk) (text 3)))
(assert (answer (ident kpk-pirat_risk_mitigation) (text "maži")))
(assert (answer (ident kpk-pirat_risk_reason) (text "kompiuterių programinės įrangos gedimai įmonei svarbūs. Gedimų vengimui naudojama piratinės programinės įrangos ir KPK apsaugos priemonės. Rizikai mažinti reikia taikyti programinės įrangos veiklos sutrikimų saugumo priemones."))))

(defrule assert-kpk-pirat-risk-33
(answer (ident irang_komp) (text taip))
(answer (ident irang_komp_v) (text ?d&:(= ?d 3)))
(answer (ident risk_mit_soft_pirat) (text taip))
(answer (ident risk_mit_kpk) (text ne))
(answer (ident risk_mit_soft) (text taip))
 =>
(assert (answer (ident kpk-pirat_risk) (text 3)))
(assert (answer (ident kpk-pirat_risk_mitigation) (text "maži")))
(assert (answer (ident kpk-pirat_risk_reason) (text "kompiuterių programinės įrangos gedimai įmonei svarbūs. Gedimų vengimui naudojama piratinės programinės įrangos ir įrangos veiklos sutrikimų saugumo priemonės. Rizikai mažinti reikia taikyti KPK apsaugos priemones."))))

(defrule assert-kpk-pirat-risk-34
```

```
      (answer (ident irang_komp) (text taip))
      (answer (ident irang_komp_v) (text ?d&:(= ?d 3)))
      (answer (ident risk_mit_soft_pirat) (text taip))
      (answer (ident risk_mit_kpk) (text taip))
      (answer (ident risk_mit_soft) (text taip))
       =>
      (assert (answer (ident kpk-pirat_risk) (text 3)))
      (assert (answer (ident kpk-pirat_risk_mitigation) (text "maži")))
      (assert (answer (ident kpk-pirat_risk_reason) (text "kompiuterių
programinės įrangos gedimai įmonei svarbūs. Gedimų vengimui naudojama
piratinės programinės įrangos, KPK ir programinės įrangos veiklos sutrikimų
apsaugos priemonės. Rizikai mažinti reikia taikyti papildomas stebėsenos
priemones.")))



      (defrule kpk-pirat-prob
      ?w <- (answer (ident tolerance) (text ?tol))
      ?x <- (answer (ident kpk-pirat_risk) (text ?t&:(>= ?t ?tol)))
      ?y <- (answer (ident kpk-pirat_risk_mitigation) (text ?kast))
      ?z <- (answer (ident kpk-pirat_risk_reason) (text ?reas))
      =>
      (printout t crlf)
      (printout t "-------------------------------------------------------
------------------------------------------------------------------------
---" crlf)
      (printout t "-------------------------------------------------------
------------------------------------------------------------------------
---" crlf)
      (printout t "
                                    " crlf)
      (printout t ">>>     Atkreiptinas     dėmesys     į     kompiuterinės
programinės įrangos gedimo rizikos mažinimą. Suskaičiuota rizika "?t", kai
nurodytas tolerancijos lygis "?tol"." crlf)
      (printout t ">>>     Rizikos mažinimo kaštai - "?kast"" crlf)
      (printout t ">>>     Tokios  rizikos  vertės  priežastis  -  "?reas""
crlf)
      (printout t "
                                    " crlf)
      (printout t "-------------------------------------------------------
------------------------------------------------------------------------
---" crlf))
```