VILNIAUS UNIVERSITETAS

KAUNO HUMANITARINIS FAKULTETAS

INFORMATIKOS KATEDRA

Verslo informacijos sistemų studijų programa

Kodas 62103S138

RITA PAULAVIČIŪTĖ

MAGISTRO BAIGIAMASIS DARBAS

DUOMENŲ APSAUGOS PRIEMONIŲ EKSPERTINĖ SISTEMA

Kaunas 2009

VILNIAUS UNIVERSITETAS

KAUNO HUMANITARINIS FAKULTETAS

INFORMATIKOS KATEDRA

RITA PAULAVIČIŪTĖ

MAGISTRO BAIGIAMASIS DARBAS

DUOMENŲ APSAUGOS PRIEMONIŲ EKSPERTINĖ SISTEMA

Leidžiama ginti _____

Magistrantas _____
(parašas)

Darbo vadovas _____
(parašas)

dr. doc. Vitolis Sekliuckis
(darbo vadovo mokslo laipsnis, mokslo pedagoginis vardas, vardas ir pavardė)

Darbo įteikimo data _____

Registracijos Nr._____

Kaunas 2009

TURINYS

SANTRAUKŲ SĄRAŠAS

1. IS – informacinė sistema.
2. DB - duomenų bazė.
3. lent. – lentelė.
4. pav. – paveikslėlis.
5. žiūr. – žiūrėti.
6. ISO – standartus suteikianti tarptautinė kompanija (International Organization for Standardization).
7. SPICE – programinės įrangos procesų pagerinimas ir pajėgumų nustatymas (Software Process Improvement and Capability dEtermination).
8. IT – informacinės technologijos.
9. ISMS - informacijos saugumo valdymo sistema (Information Security Management System).
10. IEC – tarptautinė elektronikos komisija (International Electrotechnical Commission).
11. RU - Rutgers universitetas (Rutgers university).
12. Mbone – tinklas, skirtas audio ir video informacijos perdavimo realiame laike Internete bandymams (multicast backbone).
13. ang. – anglų.
14. k. – kalba.
15. pan. – panašiai.
16. sav. – savaitė.
17. proc. – procentai.
18. el. paštas – elektroninis paštas.
19. žm. – žmogus.
20. sk. – skaičius.

PAVEIKSLŲ SĄRAŠAS

LENTELIŲ SĄRAŠAS

PAULAVIČIŪTĖ, Rita. (2009) The Expertise System for Information Security. MBA Graduation Paper. Kaunas: Vilnius University, Kaunas Faculty of Humanities, Department of Informatics. 70 p.

SUMMARY

The theme of the Master's degree paper is The Expertise System for Information Security. The object of this job is the implement for data security.

The main goal of the paper is creation the expertise system for evaluation data security, which are in computer and recommend what to do that security level of the data will be biggest. The main tasks to reach this goal are: to know the ways how security of the computer system can be impinging and how to protect from it, to do analysis trying to know what methods of data security are usable at the moment, the design of expertise system and implementation of it using C++ programme language, new system's testing and the writing user's manual.

While writing the paper, various methods, such as induction and deduction, data comparison method, generalization method were used.

During the period of implementation practical part of the work completed all main tasks. The developed software allows to know the security level of the data which are in the computer and to know the ways how to expand this level.

The main advantages of new system are: user in very quick way can know how reliable data are in the computer and he also could know the ways how to make data security level more reliable.

The length of this paper is 70 pages; there are 71 pictures (60 in extra part of this paper) and 15 tables (1 in the extra part of this paper) in this paper.

ĮVADAS

Duomenų saugumo kompiuterinėse sistemose klausimais domisi vis daugiau specialistų. Šis klausimas tampa vis aktualesnis, dėl noro apsaugoti vertingą informaciją, esančią kompiuteryje. Didėjantys vertintos informacijos kiekiai verčia kompiuterių vartotojus priimti atsakingus sprendimus norint užtikrinti kompiuterinėse sistemose laikomų duomenų saugumo lygį. Svarbi kompiuterinių sistemų vartotojų problema - konfidencialios informacijos vartojimo bei apdorojimo saugumas. Magistriniam darbui pasirinkta sukurti ekspertinę sistemą, kuri įvertintų kompiuterio saugumą ir pasiūlytų reikiamas duomenų apsaugos priemones saugumo lygio padidinimui.

Darbo tema aktuali tuo, kad duomenų apsaugos sistemų patikimumo įvertinimas - tai viena iš opiausių problemų su kuria susiduria IT specialistai. Duomenų apsaugos sistemų patikimumo įvertinimas yra galimas pagal įvairius metodus (kelis iš jų darbe apžvelgsime), bet nėra priimto vieningo duomenų apsaugos vertinimo metodo, tad susiduriama su problema, kad skirtingais metodais įvertinta ta pati kompiuterinė sistema yra vertinama skirtingai.

Kompiuterinių duomenų saugumo klausimą tyrinėjo Sh. A BUTLER, pasiūlęs išlaidų bei gaunamos naudos metodą. Remiantis šiuo metodu sistema yra tiriama nagrinėjant, kiek piniginės žalos gali padaryti duomenų esančių kompiuteryje išgadinimas. Rutgers universitetas siūlo riziką skaidyti į tris dalis: konfidencialumo, vientisumo bei verslo žlugimo. Iki šiol nėra priimto vieningo sprendimo, kaip įvertinti duomenų saugumo lygį, tad tyrinėjimai šioje srityje bus tęsiami ir ateityje.

Darbo objektas – duomenų saugos priemonės.

Darbo tikslas: sukurti ekspertinę sistemą, kuri įvertintų kompiuterinių duomenų apsaugos priemonių rinkinio saugumo lygį ir teiktų rekomendacijas saugumo lygio padidinimui.

Šiam tikslui įgyvendinti išsikelti šie uždaviniai:

- išnagrinėti rizikos faktorius bei apsaugos būdus,
- analizuoti duomenų apsaugos sistemos įvertinimo metodus,
- pasiūlyti, sukurti ekspertinę sistemą, įvertinančią duomenų apsaugos priemonių rinkinio patikimumo lygį,
- realizuoti sistemos prototipą, orientuotą į atskiro kompiuterio naudojamų saugos priemonių įvertinimą
- testuoti bei įvertinti sukurtos sistemos rezultatus.

Darbą sudaro trys pagrindinės dalys: teorinė dalis, metodinė dalis bei eksperimentinis tyrimas. Pirmojoje darbo dalyje apžvelgti metodai, kurių pagalba galima įvertinti kompiuterinės sistemos saugumą, antroje darbo dalyje apibrėžta, kas yra ekspertinė sistema ir atsakyta į klausimą, kodėl būtų labai pravartu, jei duomenų saugumo lygį esantį kompiuteryje būtų galima vertinti

ekspertinės sistemos pagalba. Paskutinė darbo dalis – tai eksperimentinė dalis, kurioje aprašyta ekspertinės sistemos, įvertinančios duomenų apsaugos priemonių saugumo lygį, projektavimo, kūrimo, testavimo eiga.

Rašant magistrinį darbą buvo parašytas bei konferencijoje „Information Technologies 2009“ (2009m. gegužės 8d.) pristatytas mokslinis straipsnis pavadinimu „Ekspertinė sistema įvertinanti duomenų saugumo lygį“ (straipsnis pateikiamas 3 darbo priede).

Darbe naudota 1999 – 2009 metų literatūra: moksliniai straipsniai, internetiniai šaltiniai, publikacijos žiniasklaidoje. Literatūros sąrašas yra sudarytas iš penkių kalbų šaltinių.

Darbe panaudoti metodai: dedukcijos metodas (naudotas temą suskaidant į smulkesnes dalis), palyginimo metodas (naudotas lyginant duomenų saugumo įvertinimo metodus), apibendrinimo metodas (naudotas apdorojant pirminę informaciją), pilnosios indukcijos metodas (naudotas rašant darbo išvadas).

Sukurta ekspertinė sistema pilnai išsprendė poreikį kompiuteriu besinaudojančiam asmeniui išsiaiškinti kompiuteryje laikomų duomenų saugumo lygį bei gauti patarimus ir pasiūlymus kaip padidinti tą lygį.

Darbą sudaro trys pagrindinės dalys, bei trys priedai. Darbo apimtis 70 psl. Darbe panaudotos: 4 formulės, 71 paveikslėliai (iš jų 60 prieduose), 15 (1 iš jų prieduose) lentelių.

1. KOMPIUTERINIŲ SISTEMŲ DUOMENŲ APSAUGOS LYGIO ĮVERTINIMO METODAI

Pirmojoje darbo dalyje yra išnagrinėti metodai, nustatantys kompiuterių sistemos duomenų saugumo lygį bei apžvelgti būdai kaip galima apsaugoti kompiuterinius duomenis.

1.1. Rizikos šaltiniai, apsaugos būdai nuo jų, metodai bei priemonės

Kompiuterinių duomenų saugumo svarba yra itin svarbi šiais laikais, kai informaciją vienas kitam vis dažniau perduodame naudodami kompiuterines technologijas, o nebe tiesioginiu būdu (gyvai bendraudami). Įmonės ar pavieniai asmenys siekdami užtikrinti informacijos konfidencialumą negaili vis daugiau lėšų ir laiko skirti kompiuterių duomenų saugumui užtikrinti.

Kompiuterinės sistemos nesaugumo šaltiniai yra šie (Ezine article, 2008 ir RFid Gazette 2007):

1. reikalavimų (būsimai IS) apibrėžimas (klaidingi, prieštaraujantys, nepilni reikalavimai),
2. sistemos konceptualumas (netinkamos technologijos taikymas, kai rizika per didelė),
3. sistemos projektavimas,
4. techninės ir programinės įrangos realizavimas (įdiegimas) (klaidos įrenginių schemose, programavimo klaidos),
5. aptarnaujančios sistemos (ribotos programavimo galimybės, klaidingi kompiliatoriai),
6. sistemos koncepcijos ir projektavimo išsamios analizės nebūvimas, kai analizė yra pagrįsta klaidingomis prielaidomis),
7. neišsami įdiegimo bei realizavimo analizė, kai nebuvo atliktas pilnas testavimas,
8. evoliucija (blogas sistemos techninis aptarnavimas, naujų klaidų įvedimas taisant senas).

Norėdami padidinti saugumo lygį kompiuterinėje sistemoje turime užtikrinti, kad prie reikiamų duomenų turi galimybę prieiti tik reikiami asmenys. Informacijai apsaugoti nuo nesankcionuoto priėjimo ir naudojimosi informacijos masyvais pagrindiniai būdai yra šie (VeriSign, 2008 ir DriveSavers Data Recovery, 2008):

1. kliūtys (kortelės, raktai, specialūs kodai),
2. kontrolė (informacijos teisėtumas, identifikavimas, autentiškumo nustatymas, įgaliojimo tikrinimas),
3. priėjimo valdymas (registruojami visi kreipiniai, ribojamas priėjimas prie informacijos masyvo),
4. informacijos pertvarkymas (siekiant užtikrinti reikiamą duomenų saugumą).

Duomenys, esantys kompiuteryje, būna saugūs tuomet, kai informacinių technologijų (toliau IT) specialistas ar kitas atsakingas asmuo yra sudaręs planą, kaip sumažinti kompiuterinei sistemai kylančias grėsmes dėl informacijos praradimo. Rekomenduojami tokie žingsniai sudarant apsaugos planą kompiuterinei sistemai (ar personaliniam kompiuteriui) (The World Wide Web Security, 2004 ir PC Tools, 2008):

1. apsaugos politika (duomenų apsauga, su ja susiję įsipareigojimai, sankcijos, apsaugos lygis),
2. esamos sistemos būsenos nustatymas (rinkos tyrimas, naujų technologijų įdiegimas),
3. rekomendacija, kaip įdiegti sistemą (rekomendacijos ką naudoti kasdieniniame darbe, ką kritinėse situacijose),
4. personalo atsakomybė (DB esančios informacijos konfidencialumas, savo slaptažodžio saugumas),
5. apsaugos priemonių įjungimo tvarka (stambias ir brangias priemones patariama diegti palaipsniui, organizuoti teorinius/praktinius užsiėmimus),
6. plano ir apsaugos priemonių sudėties peržiūrėjimo tvarka (būtina numatyti sąlygas ir terminus).

Analizuojant saugumo problemas, buvo nustatyta, kad siekiant tinkamai apsaugoti kompiuteriuose esančią informaciją reikia išnagrinėti ir įvertinti šiuos aspektus (GORDON, S., 2004 ir DRG, 2007):

1. galimos grėsmės ir rizikos analizė,
2. inventoriaus būklės įvertinimas,
3. organizacinis reagavimas, kilus nesklandumams,
4. informacijos svarbumas ir brangumas,
5. įvertinimas galimų nuostolių sutrikus kompiuterinės sistemos veiklai,
6. saugumo kriterijų parinkimas ir patikimos apsaugos sistemos apibūdinimas.

Programos (-ų) įvertinimas gali būti atliekamas atsižvelgiant į šiuos kriterijus (DRG (Data Recovery Group, 2007 ir Freepatentsonline, 2009):

1. reikalavimai kompiuterinei technikai,
2. įdiegimo ir derinimo sudėtingumas (kiek laiko trunka įdiegimo procesas, ar turimi darbuotojai sugebės įdiegti programą),
3. palankumas vartotojui (programos lankstumas ir galimybė pritaikyti individualiems vartotojo poreikiams),
4. suderinamumas su įvairiomis operacinėmis sistemomis ir kitomis kompiuteryje įdiegtomis programomis,
5. suteikiamos apsaugos lygis (vertinamas patikimumas bandant įvairius apsaugos apėjimo būdus: neveiksminga, dalinai veiksminga, saugos spragų nerasta ir pan.).

6. tinkamumas realaus laiko ir kritinėse sistemose (sistemos, kurių veikimo nutraukimas gali sukelti didelius finansinius nuostolius ar net žmonių žūtis), nuolatiniam darbui ar tik namų vartotojui ir panašiai,
7. įdiegimo ir palaikymo kaina (ar reikalingi darbuotojų apmokymai ir jei taip kiek jie kainuoja, kokia programos kaina, įdiegimo kaina).

Norint užtikrinti kompiuterinės sistemos saugumą būtina atsižvelgti į tris pagrindines priemones padedančias sukurti ir palaikyti saugią IS (Amazon, 2008, Lehigh University, 2009):

1. techninės, programinės apsaugos priemonės (techninės įrangos išdėstymas, kompiuterinių tinklų saugus išdėstymas, jų priežiūra),
2. infrastruktūrinės priemonės (pastatų, kuriuose yra kompiuterinė sistema saugumas),
3. administracinės priemonės (ar patikimas asmuo yra atsakingas už IS priežiūrą, ar duomenys saugomi keliose laikmenose, ar užtikrinama programinės įrangos apsauga it t.t.).

Išsiaiškinus, kad naudojama kompiuterinė sistema nėra saugi arba norint padidinti duomenų saugumą reikia atkreipti dėmesį į šiuos informacijos pertvarkymo būdus (ŠILKONAS, G., 2009, Nr. 5 (129), p. 32-33):

1. informacijos slėpimas („maskavimas“),
2. nematomi pakeitimai,
3. kodavimas.

Vienas iš informacijos apsaugos būdų yra informacijos slėpimas. Populiariausias informacijos slėpimo būdas yra steganografija (Blekinge Tekniska Hogskola, 2009). Jos tikslas paslėpti duomenis kitame duomenų šaltinyje, kuris dažniausiai yra vadinamas informacijos nešėju. Duomenys slepiami naudojant kodavimo algoritmą ir viešąjį raktą, kurie patalpinami į slepiamos informacijos nešėją.

Jei kompiuteriu dirbama ne tik vietiniame tinkle, bet jis turi prieigą ir į internetą, būtina pasirūpinti papildoma kompiuterio apsauga (JAMUKOWICZ, S., KOWAL, T., KWIECIEN, A., 2003). Reikėtų, kad kompiuteryje būtų įdiegtos ugniasienės. Ugniasienė - tai sistema ar net sistemų grupė, užtikrinanti saugumą tarp dviejų duomenų srautų, ateinančių iš „išorės“ į tinklų „vidų“ ir užkertanti kelią neteisėtam priėjimui į privatų tinklą arba iš privataus tinklo (YAKARIS, D., 2009, Nr. 112 (5575), p. 9).

Be aukščiau išvardintų ugniasienės privalumų, išskiriami šie ugniasienės trūkumai (Mbone, 2008 ir SecureWorks, 2009):

- egzistuoja potencialus duomenimis paremtų atakų pavojus, (kai yra bandoma pakeisti priėjimo prie resursų teises ar tiesiog svarbius failus),

- Mbone (ang. k. *multicast backbone*) (ugniasienė paprastai perduota paketus jų nenagrinėdami. Mbone pagrįsti perdavimai gali sukelti pavojų, nes juose esančios komandos gali keisti saugumo sistemos parametrus ir įsileisti įsibrovėlius),
- virusai (ugniasienė neapsaugo nuo virusais užkrėstų suarchyvuotų programų naudojimo ar jų gavimo el. paštu),
- pralaidumas (ugniasienė - tai potenciali galimybė kamščiams susidaryti jei ugniasienė greitis nėra pakankamas),
- ugniasienė sukoncentruoja tinklo saugumo priemones viename taške. Ugniasienės veikimo principas gali būti „pražūtingas“ kitoms mažiau apsaugotoms sistemoms esančioms potinklyje.

Apibendrinimas. Kompiuterinių duomenų saugumo svarba yra itin svarbi šiais laikais, kai informaciją vienas kitam vis dažniau perduodame naudodami kompiuterines technologijas. Yra labai svarbu žinoti kompiuterinės sistemos nesaugumo šaltinius, nes juos identifikavus galima imtis konkrečių veiksmų didinant saugumo lygį kompiuterinėje sistemoje.

1.2. Duomenų apsaugos sistemų patikimumo įvertinimas

Šiame poskyryje apžvelgsime duomenų saugumo įvertinimo būdus (išsiaiškinsime metodo taikymo specifiką bei išanalizuosime metodo duomenų saugumo apskaičiavimo metodiką).

1.2.1. Tradicinis rizikos analizės metodas

Kaip teigiama 2004m. pristatytoje ataskaitoje „Reaguojant į netikėtumus“ (ang. k. *Responding to the Unexpected*) (MEHROTRA, S., BUTTS, C, KALASHNIKOV, D., VENKATASUBRAMANIAN, N., 2004), tradicinė rizikos analizė – tai netikėto įvykio atsitikimo ir jo pasekmių tikimybės matavimas. Paprastesniais terminais, jei

R = rizika,

P = apytikriai įvertinta kritinio įvykio tikimybė,

C = kaina susijusi su įvykiu,

tada apytikriai įvertinta rizika yra

$$R = P * C \qquad (1)$$

Tačiau čia susiduriama su konkrečiam ir tiksliam įvertinimui kliudančiomis problemomis, nes „kaina“ gali turėti daug formų: pinigai (eurai, litai ar kita valiuta), prarastos gyvybės, gyvenimo paaukoti metai, prastovos valandų skaičius ir kt. (Softweare Quality, 2008).

Rizika R yra „laukiama reikšmė“, o priimant sprendimus ir planuojant veiklą paprastai pageidaujama visos galimos rizikos grėsmės apskaičiavimo. Su paprastu tikėtinos reikšmės apibrėžimu, 7.5 balo pagal Richterio skalę žemės drebėjimo metinė tikimybė yra $P = 10^{-2}$ ir apytiksliai įvertintas prarastų gyvybių skaičius $C = 100$ mirčių, taigi šio žemės drebėjimo rizika lygi būtų:

$$R = 10^{-2} * 100 = 1 \quad (2)$$

Arba kitas pavyzdys: apskaičiuokime 1 km skersmens meteorito atsitrenkimo į žemę ir sunaikinimo pusės planetos populiacijos riziką. Jei (taikome prielaidą) tokio įvykio tikimybė, bet kuriais duotais metais yra $0.33 * 10^{-9}$. Pusė žemės populiacijos yra apie 3 milijardai žmonių $= 3 * 10^{9}$.

Taigi tikėtina šio įvykio rizika lygi:

$$R^{*} = (0.33 * 10^{-9}) * (3 * 10^{9}) = 1 \quad (3)$$

Žemės drebėjimo ir meteorito nukritimo gautos rizikos yra lygios savo matematine išraiška, tačiau pastangos planuoti ir kovoti su šiais įvykiais labai skiriasi, Todėl tikėtinos rizikos skaičiavimai patys savaime gali būti riboti ir klaidinantys, kuriant saugumo strategiją. Taigi net ir atrodytų tikslūs ir konkretūs skaičiavimai sukelia problemų bandant įvertinti duomenų praradimo ar sugadinimo rizikos lygį (Earth and Planetary Science Letters, 2008 ir БУДИК, А., 2009).

Apibendrinimas. Tradicinis rizikos vertinimo metodas išsiskiria savo paprastumu, dėl to yra plačiai naudojamas, nes galimos reikšmės yra lengvai modeliuojamos. Tačiau skaičiuojant sistemos saugumą remiantis šiuo metodu susiduriama su neapibrėžtumu, nes kaina gali turėti daug formų: tiek pinigine išraiška, tiek prarastas laikas ir pan. Tad remiantis šiuo metodu gaunami rezultatai yra gana subjektyvūs.

1.2.2. Kompiuterinio saugumo įvertinimas pagal ISO standartą

Informacijos saugumo valdymo sistema yra skirta valdyti organizacijos IT saugumo mechanizmui. ISO 15504 standarto reikalavimuose informacijos saugumo valdymo sistemos įgyvendinimas buvo įtraukas į procesų informacinį modelį. Vykdant procesų veiklas, kurios yra aprašytos procesų informaciniame modelyje yra pasiekiamas tam tikras lygis (pagal ISO 15504 standartą - tai būtų pirmas lygis). Proceso tobulinimo bei kokybės įrankiai taip pat yra įtraukiami į valdymą. Ne kiekviena organizacija turi galimybių ir resursų sukurti pilnavertišką informacijos saugumo valdymo sistemą, ypač tos organizacijos, kurių pagrindinė veikla nėra tiesiogiai priklausoma nuo IT. Dėl to buvo apibrėžtas procesų įgyvendinimo modelis su aiškiomis sąvokomis, įgyvendinant saugumo procesus organizacijoms (ISO 27001 Security, 2008).

Kiekvienas aukštesnis lygis priartina organizaciją prie visapusiško informacijos saugumo valdymo. Paskutiniame (aukščiausiame pagal ISO standartą) lygyje yra pilnai sukuriama ir įgyvendinama informacijos saugumo valdymo sistema. Kad būtų pasiektas kuris nors lygis, organizacija turi atitikti konkrečius kriterijus, apibrėžtus procesų informaciniame modelyje. Kai organizacija atitinka visus konkretaus saugumo lygio kriterijus, ji gali bandyti įgyvendinti sekantį lygį (The Engineering ToolBox, 2005).

Remiantis ISO standartu organizacijos gali apibrėžti saugumo veiklas ir transformuoti jas į struktūras, kurių saugumo lygis yra aukštas. Yra susiduriama su saugumo procesų kokybės įvertinimo ir optimizavimo problema ir tuomet reikėtų remtis ISO 15504 standartu, kuris padeda organizacijoms išmatuoti ir įvertinti programų sistemų procesų brandą, pagal gebėjimo lygius. ISO 15504 standartas – dar kitaip vadinamas SPICE yra struktūra skirta įvertinti procesams. Procesai gali būti suskirstyti į kategorijas: pirkėjo – pardavėjo, gamybos, antraeiliai, valdymo, organizavimo. (Dorling, A., 2008 ir Шнайер, Б., 2003). Kiekvienam procesui ISO/IEC 15504 standartas atibrėžia jo pajėgumo lygį (žiūr. 1 lent.).

1 lentelė

Proceso pajėgumo lygis pagal „ ISO/IEC 15504 “ standartą

Lygis	Proceso pavadinimas
5	Optimizuojantis procesas
4	Numatomas procesas
3	Nusistovėjęs procesas
2	Valdomas procesas
1	Įvykdytas procesas
0	Neužbaigtas procesas

Šaltinis: sudaryta darbo autorės.

Kiekvieno proceso pajėgumas yra nustatomas naudojant proceso atributus. Tarptautinis standartas išskiria devynis proceso atributus (žiūr. 2 lent.).

2 lentelė

Proceso atributai pagal „ ISO/IEC 15504 “ standartą

Įvertinimo lygmuo	Atributo pajėgumas
5.2.	Proceso optimizavimas
5.1.	Naujovių diegimas į procesą
4.2.	Proceso kontroliavimas
4.1.	Proceso įvertinimas
3.2.	Proceso komponenčių žinojimas
3.1.	Proceso aiškumas
2.2.	Darbo proceso valdymas
2.1.	Atlikimo valdymas
1.1.	Proceso atlikimas

Šaltinis: sudaryta darbo autorės.

Kiekvienas proceso atributas yra detalizuojamas praktiškais rodikliais padedančiais įvertinti nagrinėjamą atributą. Kiekvienas proceso atributas yra vertinamas pagal keturių punktų vertinimo skalę (žiūr. 3 lent.) (Dorling, A., 2008).

3 lentelė

Proceso atributai pagal „ ISO/IEC 15504 “ standartą

Vertinimo kriterijus	Vertinimo skalė
Nepasiekta	0 - 15%
Iš dalies pasiekta	>15% - 50%
Didžiąja dalimi pasiekta	>50%- 85%
Pilnai pasiekta	>85% - 100%

Šaltinis: sudaryta darbo autorės.

Vertinimo rezultatai pagal ISO standartą yra pripažįstami globaliu mastu, todėl tai yra svarbus kriterijus vertinant skirtingas organizacijas (Kuhn, M., 1999). ISO 15504 standarte yra aiškiai apibrėžiama proceso sąvoka ir pateikiamas proceso vertinimas. Tai leidžia apibrėžti ISMS su aiškia struktūrine galimybe, įvertinti saugumą pagal kokybės kriterijus (Scribd, 2009).

ISO/IEC 15504 nėra metodologija ir remiantis juo darbų seka kaip teisingai vystyti projektą kompiuterinės saugos srityje nėra pateikiama. Norintiems išsamiai susipažinti su saugomo vertinimu pagal ISO standartą yra rengiami kursai. Kursai, kuriuose yra paaiškinama ISO standartų kvalifikacija, kainuoja 2500 eurų vienam asmeniui (kursai rengiami D. Britanijoje, Italijoje, Prancūzijoje, Japonijoje) (eSecurity, 2006).

Apibendrinimas. ISO standartas - tai tarptautinis standartas, kuris kompiuterio saugumą vertina pagal jame vykstančius procesus, procesai savo ruoštu yra skirstomi į atributus, o atributai turi kelis įvertinimo lygmenis. Tokia kompiuterinio saugumo vertinimo metodika yra patikima ir ja remiantis organizacijos gali apibrėžti saugumo veiklas ir transformuoti jas į saugias struktūras.

1.2.3. Saugumo klasės pagal „Oranžinę knygą“

„Oranžinėje knygoje“ (plačiau 4 lent.) apibrėžiami keturi saugumo lygiai (A, B, C, D, kur A klasė – tai aukščiausia saugumo klasė). Lygis D skirtas nesaugioms sistemoms, kurioms nekeliami jokie saugumo reikalavimai. Lygiai C ir B yra skirstomi į klases: C1, C2, B1, B2, B3, A1 (Voting Matters, 2000). Kiekvienai klasei taikomus reikalavimus galima suskirstyti į tokias grupes:

- reikalavimai kreipinių valdymo sistemai,
- reikalavimai registracijos ir apskaitos sistemai,
- reikalavimai vientisumo užtikrinimui (Electronic Orange Book, 2008).

4 lentelė

Saugumo klasės pagal „Oranžinę knygą“

Saugumo grupė	Apibūdinimas
D (minimali apsauga)	Kompiuterinės sistemos, netenkinančios saugumo reikalavimų, keliamų aukštesnėse klasėse.
C (diskretiška apsauga)	Turi apsaugos priemones, naudojamas vartotojo, įskaitant ir bendras kontrolės priemones ir subjektų bei jų veiksmų apskaitą.
C1 (diskretiška apsauga)	Apima sistemas su išskiriamais vartotojais ir duomenimis.
C2 (valdomo priėjimo apsauga)	Apima sistemas, užtikrinančias aukštesnes apsaugos priemones, negu klasėje C1, kurios individualiai išskiria vartotojus įvedimo procedūroj ir įvykių, susijusių su sistemos apsauga ir duomenų izoliacija, valdyme.
B (įgaliota apsauga)	Yra trys klasės (pateiktos žemiau).
B1 (žyminė apsauga)	Tenkina visus C2 klasės reikalavimus, papildomai realizuojančios iš anksto numatytą apsaugos modelį, palaikančias objektų, subjektų žymes, visišką priėjimo kontrolę.
B2 (struktūrizuota apsauga)	Aiškiai apibrėžiamas ir dokumentuotos apsaugos užtikrintas formalizuotas modelis, o priėjimo išskyrimo ir kontrolės žymių mechanizmas, paskirstytas visiems vartotojams, duomenims bei visiems priėjimo būdams.
B3 (apsaugos sritis)	Šios klasės sistemose turi būti mechanizmas, kuris registruotų visų rūšių priėjimus prie bet kurio objekto. Šios klasės sistemos turi turėti priemones ryšio palaikymui su apsaugos administratoriumi.
A (tinkama apsauga)	Sistemų realizuotų apsaugos priemonių tikrinimui naudojami formalūs metodai. Reikalaujama, kad būtų pilna sistemos projektavimo, vystymo ir vartojimo dokumentacija.
A1 (tinkamas išskyrimas)	Funkcionaliai adekvačios B3 saugumo grupei ir nereikalaujančios kokių nors papildomų priemonių. Sistemos turi turėti galingas konfigūracijos ir apsaugos administratoriaus palaikymo priemones.

Šaltinis: sudaryta darbo autorės.

Metodo trūkumas: klasės išskiriamos tiktai keturios, o dažniausiai aptinkamos kompiuterinės sistemos pasiskirsto tarp dviejų klasių (B ir C), nėra išvengiama subjektyvaus vertinimo, nes saugumo klasėje nėra apibrėžti visi galimi kompiuterinės sistemos komponentai (TREACY, B. C., 2007).

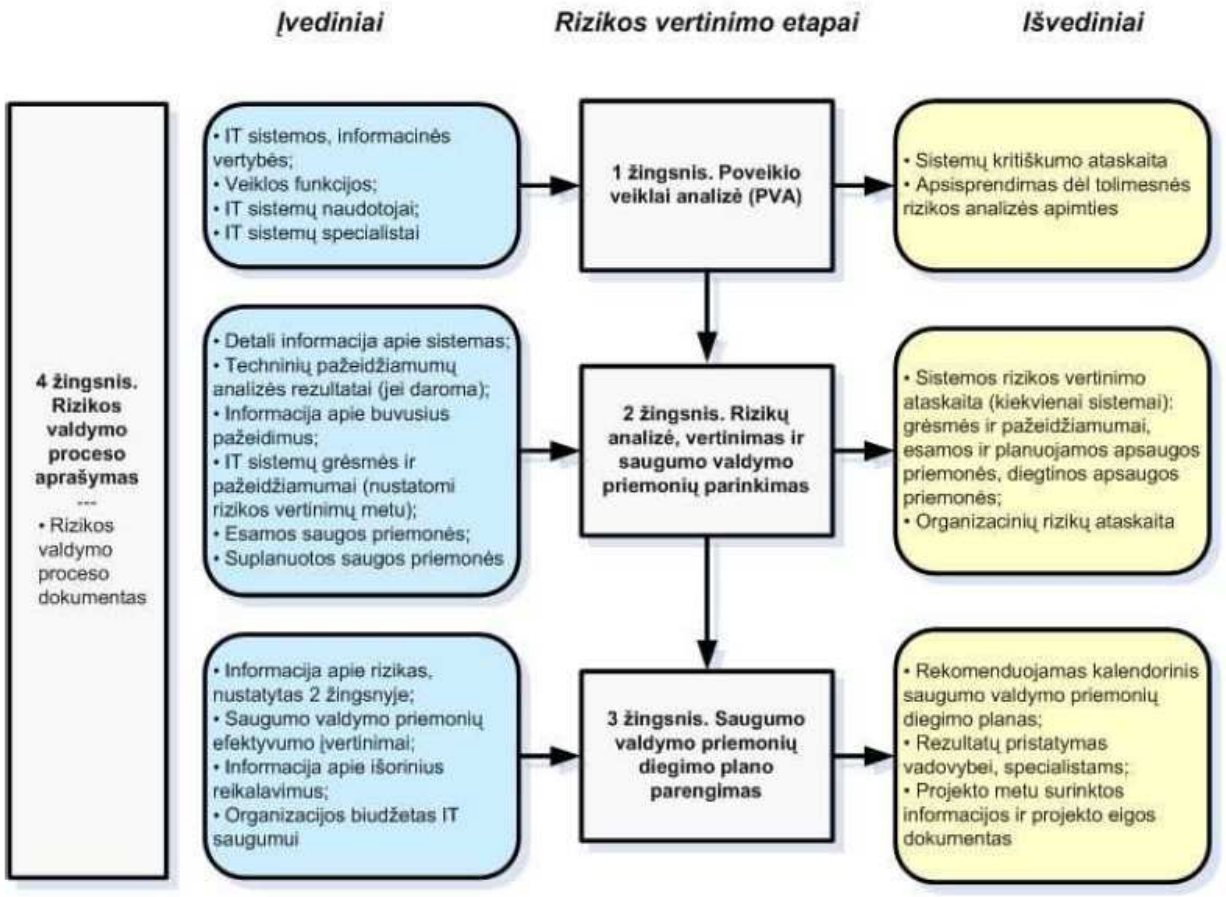
Apibendrinimas. Saugumo klasių klasifikacija pagal „Oranžinę knygą“ pasižymi aiškumu ir apibrėžtumu, bet vertinant kompiuterinę sistemą neišvengiama subjektyvumo, nes perėjimas tarp

klasių nėra išsamiai apibrėžtas. Metodologija yra pritaikyta vertinti kompiuterinius tinklus, o ne pavienius kompiuterius.

1.2.4. Rizikos įvertinimas pagal “Informacijos saugos sprendimus”

Organizacijos UAB „Informacijos saugos sprendimai“ pagrindinė veikla yra konsultacijos, mokymai, auditas, susijęs su informacijos sauga. Ši kompanija yra parengusi rizikos įvertinimo metodiką. Rizikos vertinimo gylis skirtingose organizacijos skiriasi, nes tai priklauso nuo įmonės veiklos specifikos bei finansinių galimybių. Norint įvertinti rizikos lygį teisingai kiekvieną kartą reikėtų atsižvelgti į konkrečios organizacijos poreikius (Informacijos saugos sprendimai, 2008 ir LEŠČINSKAS, L., 2009, Nr. 6 (85), p. 46-49).

Rizikos vertinimo procesą būtų galima išskirti į keturis pagrindinius etapus (žiūr. 1 pav.):



Šaltinis: Informacijos saugos sprendimai (2008) <www.isec.lt>.

1 pav. Rizikos vertinimo proceso pagrindiniai etapai

Poveikio veiklai analizė įvertina kiek organizacijai yra svarbios informacinės sistemos bei kurios iš šių sistemų yra svarbiausios. Tai yra įgyvendinama šiais būdais: informacija surenkama interviu metodu dažniausiai iš organizacijos vadovų ar kitų patyrusių darbuotojų. Surinkta medžiaga yra dokumentuojama taip, kad prireikus ja būtų galima pasinaudoti po metų ar vėlesniu

laikotarpiu. Išanalizuojami poveikio veiklai rezultatai ir pateikiama informacija kokie sistemos aspektai yra labiausiai reikalaujantys detalaus tyrimo bei kurios vietos organizacijoje yra mažiausiai apsaugotos.

Rizikos analizės, vertinimo bei saugumo valdymo priemonių pasirinkimo etape nustatoma ir įvertinama organizacijos informacinės sistemos, pagrindinės joms kylančios grėsmės, rekomenduojamos saugumo valdymo priemonės. Tyrimo metu gali būti naudojami metodai analogiški kompiuterių įsilaužėlių (ang. k. *hacker*) naudojamiems metodams. Šio etapo įgyvendinimas: imamas interviu iš informacinių technologijų specialistų, kad būtų teisingai išanalizuotos organizacijos informacinei sistemai gresiančios rizikos. Taip pat atliekamas interviu su organizacijos atstovais, kurie žino darbų atlikimo tvarką bei eigą. Atliekama dokumentacija taip, kad prireikus ja būtų galima pasinaudoti po metų ar vėlesniu laikotarpiu. Saugumo priemonės parenkamos remiantis ISO/IEC 27001, ISO/IEC 17799:2005 tarptautiniais standartais. Jei organizacija apsisprendžia sumažinti rizikos lygį yra parenkamos techninės ar organizacinės priemonės padedančios tai įgyvendinti (GIMŽAUSKAS, G., 2009, Nr. 5, p. 20-22 ir Informacijos saugos sprendimai, 2008).

Svarbiausi veiksniai parengiant saugumo vykdymo priemonių diegimo planą yra: rizikos lygio nustatymas; sprendimų radimas, kas galėtų padėti efektyviai sumažinti rizikos lygį; išsiaiškinimas organizacijos skiriamų lėšų dydžio, turimų žinių, žmonių, laiko sprendimų diegimui bei priežiūrai (ar jie pakankami); išsiaiškinimas ar organizacija turi atitikti specialius teisinius reikalavimus , kokia yra pirkimo procedūrų specifika ir t.t. Visa tai yra įgyvendinama analizuojant praeituose etapuose sudarytas ataskaitas ir bendraujant su atsakingais organizacijos vadovais sudaromas saugumo valdymo priemonių diegimo planas (JAKAS, D., 2008, Nr. 11 (227), p. 10).

Priklausomai nuo organizacijos dydžio rizikos analizės procese gali dalyvauti daug dalyvių, tad yra labai svarbu išanalizavus silpniausias organizacijos vietas sudaryti planą (kalendorinį tvarkaraštį), kuriame atsispindėtų kas ir kada yra atsakingas už tam tikrų sprendimų atlikimą/ priežiūrą mažinančių rizikos kiekį organizacijoje (Informacijos saugos sprendimai, 2008).

Apibendrinimas. Rizikos įvertinimas remiantis „Informacijos saugos sprendimai“ siūloma metodika susideda iš šių etapų: poveikio veiklai ir rizikos analizė, saugumo vykdymo priemonių diegimo plano sudarymas bei rizikos valdymo proceso dokumentas. Tyrimo šiuo metodu galutinis tikslas yra pateikti planą (kalendorinį tvarkaraštį), kuriuo remiantis atsispindėtų kas ir kada yra atsakingas už tam tikrų sprendimų atlikimą/ priežiūrą mažinančių rizikos kiekį organizacijoje.

1.2.5. „RU Security“ siūlomas rizikos vertinimo metodas

Riziką siūloma skirstyti į tris klases pagal „RU Security“ (Rutgers universiteto pasiūlytas duomenų saugumo lygio nustatymo metodas):

- konfidencialumo rizika,
- duomenų vientisumo rizika,
- prieinamumo arba verslo žlugimo rizika (DUNCAN, G. T., KELLER-MCNULTY, S. A., ir STOKES, S. L., 2004).

Konfidencialumo rizika nurodo neautorizuoto priėjimo prie informacinių išteklių (tokių kaip kliento informacija, slaptažodžiai, studentų pažymiai, tyrimų duomenys ir t.t.) įtaką. „RU Security“ siūlomas konfidencialumo ir vientisumo rizikos vertinimo metodas pateiktas 5 lentelėje.

Duomenų vientisumo rizika apibūdina netikslių duomenų naudojimo riziką, netinkamiems verslo ar valdymo sprendimams priimti. Ši rizika taip pat nurodo įtaką, jei kliento informacija, tokia kaip studentų pažymiai ar sąskaitų balansai būtų neteisingi, ar netikslūs duomenys naudojami tyrime, ar nusiųsti tretiesiems asmenims. Netikslių duomenų perdavimas klientams, akcininkams, visuomenei ir t.t. gali sukelti verslo praradimą, teisinį procesą, ar klientą paveikti morališkai (pvz. jei jis bus viešai pažemintas) (Rutgers secure. Risk Assessment, 2008).

5 lentelė

„RU Security“ siūlomas konfidencialumo/vientisumo rizikos vertinimas

Informacijos konfidencialumas	Tikimybė	Sugadinimo įtaka	Saugumo lygis (Tikimybė + Įtaka = Saugumo lygis)
Jei saugote slaptą informaciją (studentų pažymius, slaptus tyrimų duomenis ar kt slaptą informaciją) kokia tikimybė, kad konfidencialumas bus pažeistas? Jei bus pažeistas, koks poveikis jums ir klientams?	o Aukšta (≥0,7) o Vidutinė (>0,3 ir <0,7) o Žema (≤0,3)	o Aukšta (≥7) o Vidutinė (>3 ir <7) o Žema (≤3)	10 × Aukšta + Aukšta = Aukšto lygio apsauga 10 × Aukšta + Vidutinė = Aukšto lygio apsauga 10 × Aukšta + Žema = Vidutinio lygio apsauga 10 × Vidutinė + Aukšta = Aukšto lygio apsauga 10 × Vidutinė + Vidutinė = Vidutinio lygio apsauga 10 × Vidutinė + Žema = Vidutinio lygio apsauga 10 × Žema + Aukšta = Vidutinio lygio apsauga 10 × Žema + Vidutinė = Vidutinio lygio apsauga 10 × Žema + Žema = Žemo lygio apsauga

Šaltinis: sudaryta darbo autorės.

Prieinamumo ar verslo žlugimo rizika apibūdina tikėtiną riziką sistemos klaidų ar nelaimės sukelto veiklos nutraukimo. Yra nagrinėjama įtaka tiek klientams tiek atskiriems veiklos sektoriams. „RU Security“ siūlomas prieinamumo ar verslo žlugimo rizikos vertinimo metodas pateiktas 6 lentelėje.

6 lentelė

„RU Security“ siūlomas prieinamumo arba verslo žlugimo rizikos vertinimas

Informacijos prieinamumas	Tikimybė	Sugadinimo įtaka	Saugumo lygis (Tikimybė + Įtaka = Saugumo lygis)
Jei esate smarkiai priklausomi nuo priėjimo prie savo duomenų, kokia yra priėjimo netekimo tikimybė? Jei bus pažeistas, koks poveikis būtų jums ir klientams?	o Aukšta (≥0,7) o Vidutinė (>0,3 ir <0,7) o Žema (≤0,3)	o Aukšta (≥7) o Vidutinė (>3 ir <7) o Žema (≤3)	10 × Aukšta + Aukšta = Aukšto lygio apsauga 10 × Aukšta + Vidutinė = Aukšto lygio apsauga 10 × Aukšta + Žema = Vidutinio lygio apsauga 10 ×Vidutinė + Aukšta = Aukšto lygio apsauga 10 ×Vidutinė + Vidutinė = Vidutinio lygio apsauga 10 ×Vidutinė + Žema = Vidutinio lygio apsauga 10 × Žema + Aukšta = Vidutinio lygio apsauga 10 × Žema + Vidutinė = Vidutinio lygio apsauga 10 × Žema + Žema = Žemo lygio apsauga

Šaltinis: sudaryta darbo autorės.

Kiekvienos rizikos klasės, kiekvieno lygio apsaugai „RU Securety“ siūlo atitinkamus apsaugos sprendimus (įsilaužimo nustatymo sistemas, ugniasienes, antivirusines sistemas, nepertraukiamo maitinimo šaltinius, slaptažodžius). Šio metodo didžiausias keblumas yra šis: kaip tiksliai nustatyti rizikos ir įtakos dydžius. Skaičiavimuose yra naudojami tik lingvistiniai terminiai „aukšta“, „vidutinė“, „žema“, tačiau kur nubrėžti ribas tarp šių dydžių (kaip žinoti, kaip priskirti galimą grėsmę, jei jo reikšmė svyruoja tarp „aukšta“ ir „vidutinė“?). Tad yra sunku įvertinti duomenų svarbą arba galimos žalos dydį remiantis šiuo metodu. Naudojantis šia metodika, tikimybes ir įtakas galima vertinti tik apytiksliai ir beveik nepagrindžiant dydžio pasirinkimo tikimybės (Rutgers secure. Risk Assessment, 2008).

Apibendrinimas. „RU Security“ metodo pagalba galima lengvai modeliuoti galimas reikšmes trijose kategorijose (konfidencialumo, duomenų vientisumo, verslo žlugimo rizikos vertinime), tačiau pastebėtina, kad gauti rezultatai yra daugiau tikėtini nei realūs (tikslūs), nes ribos tarp reikšmių „aukšta“, „vidutinė“, „žema“ nėra apibrėžtos, o yra nustatomos subjektyviai.

1.2.6. Saugumo požymių įvertinimo metodas: išlaidų ir gaunamos naudos

Nagrinėjant saugumo požymių įvertinimo metodą paremtą išlaidomis ir gaunama nauda yra analizuojama kompiuterinė sistema. Šis metodas yra naudingas palyginti alternatyvius saugumo projektus finansiškai ir duodamos naudos atžvilgiu.

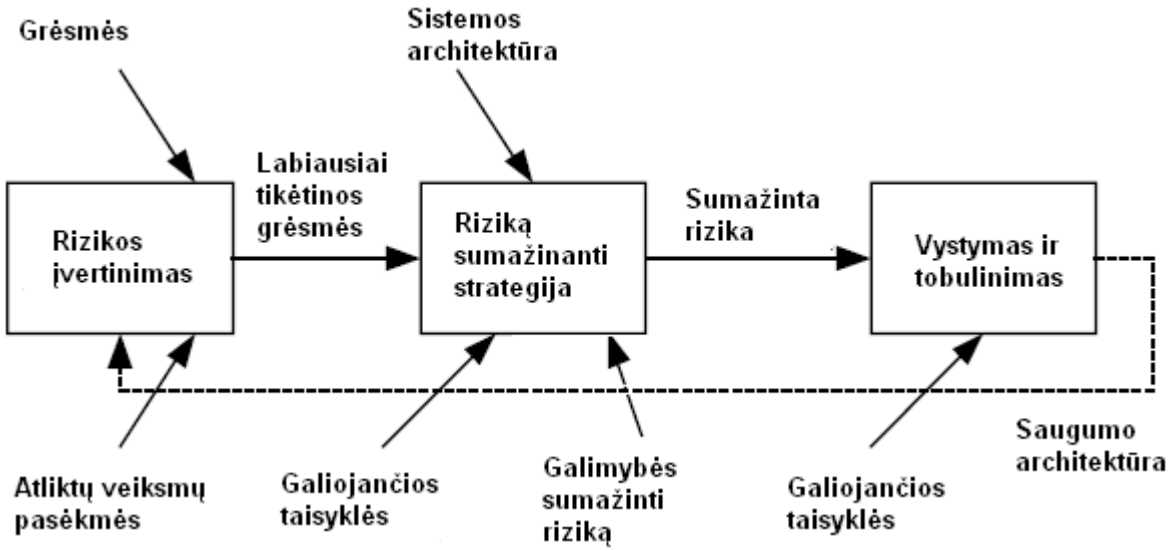
Naudojant šį metodą alternatyvos yra palyginamos su šiuo metu organizacijos pasirinkta saugumo sistema įsitikinti ar efektyvesnis pinigų panaudojimas saugumo srityje yra galimas. Bet technologijos yra visad sunkiai įvertinamos, todėl IT specialistai visad turi keblumų nustatydami alternatyvas. Saugumo technologijų nešama nauda priklauso nuo to, kaip dažnai ataka yra tikėtina, kiek daug žalos gali padaryti ir kaip efektyviai saugumo technologijos gali sumažinti atakų daromą žalą. IT specialistai yra suinteresuoti išgauti didžiausią saugumo lygį minimaliai tam išleidžiant. Šis

metodas tik įvertina technologijų kombinavimo galimybes, bet ne rizikos sumažinimo procedūras (BUTLER, Sh. A., 2002).

Schemoje pateiktas saugumo sandaros vystymo procesas, kuris prasideda (Von HIPPEL, E., 2007):

1. nuo rizikos įvertinimo, kurio metu yra įvertinamos grėsmės bei atliktų veiksmų pasekmės,
2. tuomet yra parenkama riziką sumažinanti strategija ir atsižvelgiant į sistemos architektūrą, galiojančias taisykles bei kokios grėsmės yra labiausiai tikėtinos šiai sistemai priimamas sekantis žingsnis,
3. sistema yra vystoma bei tobulinama ir jei reikia vėl grįžtama į pirmą punktą, kad būtų įvertinta gresianti rizika.

Praktikoje procesai yra komplikuoti todėl, kad rizikos įvertinimo duomenys yra paremti apsauga besirūpinančio žmogaus subjektyvaus požiūrio ir išprusimo lygio (žiūr. 2 pav.).



Šaltinis: sudaryta darbo autorės.

2 pav. Informacinės sistemos saugumo sandaros vystymo procesas

Nors firmos darbuotojai palieka saugumo klausimus spręsti saugumo specialistams, jie dažnai nerimauja ar investavimas į saugumą yra kryptingas ir teisingas. Rizikos įvertinimo tikslas yra nustatyti grėsmes ir jų įtaką sistemai po sėkmingos atakos taip, kad IT specialistas galėtų surūšiuoti juos pagal svarbą.

Rizikos valdymo, paremto kelių grėsmių valdymu, analizė siūlo patogią struktūrą nustatančią grėsmių sistemoje pralaidumą. Tradiciškai yra naudojama sprendimų priėmimo srityje išbandant konkrečių atakų prasiskverbimo į sistemą grėsmę.

Rizikos valdymas paremtas kelių grėsmių valdymu susideda iš keturių etapų:

1. pirmame etape IT valdymo ir saugumo specialistas identifikuoja įeinančius atributus (produktyvumas, grįžtamumas, reputacija, pažeidimo bauda),
2. tuomet yra įvardijamas dažnumas ir įeinančių atributų vertės kiekvienai grėsmei,
3. IT specialistas identifikuoja atributų vertes bei jų įtaką kitiems sistemos komponentams,
4. galiausiai, grėsmių duomenys ir atributų išrikiavimas yra naudojamas sugeneruoti grėsmių indeksui (BUTLER, Sh. A., 2002).

IT specialistas apskaičiuoja, kad tikimybė patirti grėsmę yra lygi nuo 2-3 kartų per valandą iki 2-3 kartų per metus. Lentelėje prarastos pajamos yra skaičiuojamos pinigine išraiška, o produktyvumo praradimas skaičiuojamas žmogaus prarastomis valandomis.

7 lentelė

Grėsmės dažnumas ir išeinančios reikšmės

Grėsmė (įvertinimas atakų per metus)		Prarastas produktyvumas (h)	Reputacija (skalėje 1-10)	Prižiūrėtojų baudos (skalėje 1-10)	Prarastos pajamos (Lt)
Skanavimas (10220)	**Žemas**	0,25	1	0	0
	Tikėtinas	0,5	1	0	0
	Aukštas	1	4	0	1000
Procedūrinis nepažeidžiamumas (4380)	**Žemas**	0	0	0	0
	Tikėtinas	2	1	0	0
	Aukštas	40	4	3	12000
Stebėjimas (2920)	**Žemas**	0	0	0	0
	Tikėtinas	0	1	0	0
	Aukštas	8	4	0	0
Sistemos vientisumo pažeidimas (156)	**Žemas**	1	1	0	0
	Tikėtinas	3	2	0	0
	Aukštas	200	3	0	0
Slaptažodžio perėmimas (365)	**Žemas**	0,5	0	0	0
	Tikėtinas	0,5	0	0	0
	Aukštas	0	0	0	0
Asmeninis piktnaudžiavimas (110)	**Žemas**	0	0	0	0
	Tikėtinas	0,17	0	0	0
	Aukštas	4	1	0	0

Šaltinis: sudaryta darbo autorės.

Po pirminio grėsmių tikimybių sudėliojimo IT specialistas įvertina grėsmes skalėje nuo 1 iki 100. Atributas keliantis daugiausiai nerimo gauna įvertinimą lygu 100 balų. Taip yra įvertinami visi atributai, galiausiai suskaičiuojamos jų vertės skalėje nuo 0 iki 1 (žiūr. 8 lent.).

8 lentelė

Atributų išrikiavimas ir svoriai

Atributai	Eiliškumas	Svoris
Prarastas produktyvumas	100	0,42
Reputacija	80	0,33
Prižiūrėtojų baudos	40	0,17
Prarastos pajamos	20	0,08

Šaltinis: sudaryta darbo autorės.

TI_a kiekvienai atakai a yra apskaičiuojama kiekvieno IT specialisto subjektyviai priskirtai vertei bei tikimybei. TI reikšmė yra įvertinimo vienetai, kurie yra skirtingi keičiantis rizikos grėsmės lygiui. Kiekviena pasirinkta atakos grėsmė apskaičiuojama atskirai įvertinant jos pasirodymo galimybę retai, kartais ir dažnai (BUTLER, Sh. A., 2002):

$$TI_a = F_a * [PŽ * (\square_{j = atributai} W_j * V_j (x_{j\ lžemas})) + PT * (\square_{j = atributai} W_j * V_j (x_{j\ tikėtina})) + PA * (\square_{j = atributai} W_j * V_j (x_{j\ aukštas}))] \quad (4)$$

Kur:

TI_a – grėsmės svoris,

P – grėsmė,

Ž – žema,

T – tikėtina,

A- aukšta,

W- svoris,

F- dažnumas,

V- vertė,

j- atributas,

a- ataka.

Žemiau pateiktoje lentelėje parodyta grėsmių indekso apskaičiavimas šešioms galimomis rizikos rūšims.

9 lentelė

Grėsmių indeksai

F_a*PŽ*PT*PA*□(Wj*$V_{(xAj*xTj*xŽj)}$)				**TI**
	Žema P=1	**Tikėtina P=0,89**	**Aukšta P=0,1**	
Skanavimas	85,61	765,88	34,95	886,44
Procedūrinis nepažeidžiamumas	0	338,39	28,59	366,98
Stebėjimas	0	216,57	10,14	226,98
Sistemos paskirstymo nepriėmimas	1,33	23,86	0,93	26,12
Slaptažodžio perėmimas	0,03	0,28	0,31	0,62
Asmeninis piktnaudžiavimas	0	0,03	0,1	0,13
Viso	86,97	1345,01	75,03	1507,00

Šaltinis: sudaryta darbo autorės.

Saugumo atributų įvertinimo metodo tikslas yra struktūrizuoti išlaidų ir gautos naudos procesą, įvertinant alternatyvias struktūras. Šis procesas apima keturis žingsnius:

1. naudos įvertinimas,
2. grėsmių indeksų nustatymas,
3. saugos įvertinimas,
4. išlaidų analizė.

Norint atlikti naudos ar efektyvumo įvertinimą sistemoje yra tiriama kaip sistema reaguoja į galimą riziką. Saugumo sistemos gedimai dažniausiai yra sėkmingai nustatomi naudojant kelias grėsmes sistemai. Sistemų, kurios ieško galimų grėsmių, pagrindinis tikslas yra nustatyti, kokia yra grėsmės tikimybė įsiskverbti į sistemą ar konstantuoti faktą, kad tai jau yra įvykę. (BUTLER, Sh. A., 2002).

Apibendrinimas. Išlaidų bei gaunamos naudos metodo rezultatais galima pasikliauti tik tuo atveju jeigu kompiuterinę sistemą vertina kvalifikuotas IT specialistas, nes suteikiama teisė pačiam specialistui įvertinti grėsmių svarbą. Jei specialistas nėra tikras savo srities žinovas - jo priimtos prielaidos vėliau paaiškės buvusios neteisingos ir organizacija bus investavusi į mažiau svarbias vietas savo informacinio saugumo užtikrinimui.

1.3. Sistemų apsaugos lygio įvertinimo metodų analizės išvados

Tradicinis rizikos vertinimo metodas išsiskiria savo paprastumu, dėl to yra plačiai naudojamas, nes galimos reikšmės yra lengvai modeliuojamos. Tačiau skaičiuojant sistemos saugumą remiantis šiuo metodu susiduriama su neapibrėžtumu, nes kaina gali turėti daug formų: tiek pinigine išraiška, tiek prarastas laikas ir pan. Tad remiantis šiuo metodu gaunami rezultatai yra gana subjektyvūs.

ISO standartas - tai tarptautinis standartas, kuris kompiuterio saugumą vertina pagal jame vykstančius procesus, procesai savo ruoštu yra skirstomi į atributus, o atributai turi kelis įvertinimo lygmenis. Tokia kompiuterinio saugumo vertinimo metodika yra patikima ir ja remiantis organizacijos gali apibrėžti saugumo veiklas ir transformuoti jas į struktūras, koncentruotas į saugumą.

Saugumo klasių klasifikacija pagal „Oranžinę knygą“ pasižymi aiškumu ir apibrėžtumu, bet vertinant kompiuterinę sistemą neišvengiama subjektyvumo, nes perėjimas tarp klasių nėra išsamiai apibrėžtas. Metodologija yra pritaikyta vertinti kompiuterines sistemas, o ne pavienius kompiuterius.

„RU Security“ metodo pagalba galima lengvai modeliuoti galimas reikšmes trijose kategorijose (konfidencialumo, duomenų vientisumo, verslo žlugimo rizikos vertinime), tačiau pastebėtina, kad gauti rezultatai yra daugiau tikėtini nei realūs (tikslūs), nes ribos tarp reikšmių „aukšta“, „vidutinė“, „žema“ nėra apibrėžtos, o yra nustatomos subjektyviai.

Rizikos įvertinimas remiantis „Informacijos saugos sprendimai“ siūloma metodika susideda iš šių etapų: poveikio veiklai ir rizikos analizė, saugumo vykdymo priemonių diegimo plano sudarymas bei rizikos valdymo proceso dokumentas. Tyrimo šiuo metodu galutinis tikslas yra pateikti planą (kalendorinį tvarkaraštį), kuriuo remiantis atsispindėtų kas ir kada yra atsakingas už tam tikrų sprendimų, mažinančių rizikos kiekį organizacijoje, atlikimą/ priežiūrą.

Išlaidų bei gaunamos naudos metodo rezultatais galima pasikliauti tik tuo atveju, jeigu kompiuterinę sistemą vertina kvalifikuotas IT specialistas, nes suteikiama teisė pačiam specialistui įvertinti grėsmių svarbą. Jei specialistas nėra tikras savo srities žinovas- jo priimtos prielaidos vėliau paaiškės buvusios neteisingos ir organizacija bus investavusi į mažiau svarbias vietas savo informacinio saugumo užtikrinimui.

2. KOMPIUTERIO DUOMENŲ APSAUGOS PRIEMONIŲ AUTOMATIZUOTO ĮVERTINIMO PRINCIPAI

Šios darbo dalies tikslas – pasiūlyti ekspertinės sistemos, leidžiančios kiekybiškai įvertinti duomenų saugumo lygį bei parenkančios rekomendacijas jo didinimui, struktūrą. Aprašyti kokiu principu bus pagrįstas kuriamos ekspertinės sistemos veikimas.

2.1. Ekspertinė saugumą vertinanti sistema

Apžvelgus keletą iš galimų metodų, kurių pagalba galima įvertinti kompiuterinę sistemą (ar pavienį kompiuterį) darytina išvada, kad metodų pagalba gaunami rezultatai dažnai yra daugiau subjektyvūs nei patikimi ir tikslūs. Norint, kad kompiuterinės sistemos saugumo įvertinimas būtų kuo efektyvesnis reikia būti tikram, kad sistemą vertina kompetentingas asmuo. Nes tik kompetentingas asmuo subjektyviai nustatydamas ribas tarp saugumo klasių (saugumo lygiai pagal „oranžinę knygą“) ar parinkdamas koeficientus įvertinančius grėsmių tikimybę (išlaidų ir gaunamos naudos metodas) mažiausiai nukryps nuo realybės, nes remsis ne spėjimais, o mokslinėje literatūroje pateikiama informacija bei praktikoje išnagrinėtais faktais.

Visos nagrinėtos metodikos yra paremtos tuo, kad fizinis ar juridinis asmuo norėdamas išsiaiškinti savo kompiuteryje laikomų duomenų saugumo lygį turi kreiptis arba į specialistą arba į organizaciją ir ji (savaime suprantama už tam tikrą mokestį, kartais net labai aukštą ISO standarto atveju) įvertina patikimumą. Įvertinimai dažnai nepateisina lūkesčių, ne todėl, kad įvertinama žemais balais, bet todėl, kad išsiaiškinus kompiuterinės sistemos saugumo lygį yra nežinoma kokių konkrečių veiksmų reikėtų imtis, kad saugumas būtų aukštesnio lygio. Dažniausiai klientui yra suteikiama tik informacija, ką daryti, kad patikimumo / saugumo lygis pereitų į kitą aukštesnį etapą.

Nuspręsta projektuoti ekspertinę sistemą, nustatančią duomenų esančių kompiuteryje saugumo lygį bei patariančią vartotojui, kokių saugumo priemonių imtis, kad duomenų saugumo lygis būtų aukštesnis. Ekspertinę sistemą dar galima vadinti žiniomis grindžiama sistema, nes ji daro išvadas iš pateiktų duomenų arba išsprendžia tam tikrus uždavinius. Ši sistema visuomet yra kompiuterinė programa. Ekspertinė sistema yra pranašesnė už duomenų bazę tuo, kad duomenų bazės tik iškviečia ir pateikia joje laikomus duomenis, o ekspertinė sistema analizuoja duomenis bei pateikia išvadas (SAYCIER, G. BELLON, C., 2006).

Nutarta kurti ekspertinę sistemą, kurios pateikiamos išvados būtų duomenų saugumo lygio įvertinimas. Ši sistema taip pat atliktų analizės funkciją: kiekviename žingsnyje (vartotojo atsakomame klausime) būtų analizuojama ir skaičiuojama ar nekyla grėsmė duomenų saugumui ir susidūrus su grėsme būtų skaičiuojama galima jos žala duomenų saugumui. Be to, susidūrus su

grėsme ekspertinė sistema taip pat patartų vartotojui, kurių priemonių reikėtų imtis, kad duomenys esantys kompiuteryje būtų saugesni. Patarimai ir rekomendacijos vartotojui butų pateikiami, tik kai jis baigia atsakinėti į klausimus nustatančius bei įvertinančius duomenų saugumo lygį.

Nuspręsta sukurti ekspertinę sistemą, kuria galėtų naudotis net pradedantysis kompiuterio vartotojas. Kuriama sistema būtų orientuota į mažai žinių apie duomenų saugumą turinčius žmones, nes darytina išvada, kad būtent jiems ekspertinės sistemos pateikiami patarimai ir rekomendacijos yra reikalingiausios, nes kompiuterių ekspertas ir be ekspertinės sistemos patarimų žino (tiksliau, žymiai geriau nei pradedantysis kompiuterio vartotojas žino), kaip užtikrinti savo duomenų, esančių kompiuteryje saugumą.

Kai buvo apsisprendžiama kokiai operacinei sistemai pritaikyti ekspertinės sistemos užduodamus klausimus, buvo pasirinkta Windows operacinė sistema (KATZ, J., MERIER, R. J., 2005). Toks pasirinkimas padarytas, remiantis tuo, kad dauguma virusų veikia Windows terpėje, nors naujausia Windows versija (Windows Vista) žengė didelį žingsnį į priekį, siekiant užtikrinti sistemos, bei joje esančių duomenų saugumą, ji vis tiek saugumo atžvilgiu yra lengviau pažeidžiame lyginant su Linux operacine sistema (SKROBIKAS, M., 2009, Nr. 9, 5 psl.).

Ekspertinės sistemos duomenų saugumo lygio apskaičiavimas turi būti paremtas tam tikra metodika. Pirmame skyriuje išnagrinėjome keletą iš jų ir negalima teigti, kad viena metodika yra geresnė, teisingesnė, svarbesnė už kitas. Tad kuriant ekspertinę sistemą reikia kurti savitą metodiką, kuri tik remtųsi kitų metodikų apskaičiavimo pagrindais. Skaičiuojant duomenų saugumo lygį nuspręsta nesiremti tradiciniu rizikos vertinimo metodu, nes skaičiuojant sistemos saugumą remiantis šiuo metodu susiduriama su neapibrėžtumu, nes kaina gali turėti daug formų: tiek piniginė išraiška, tiek prarastas laikas ir pan. Deja, negalima nekreipti dėmesio, kad apskaičiuojant kompiuterinės sistemos saugumą tradiciniu rizikos apskaičiavimo metodu yra susiduriama su subjektyviu vertinimu, tad nežinant kas vertins kompiuterinę sistemą (ar tikrai vertinantis asmuo bus pakankamai kompetentingas tiriamojoje srityje) negalima teigti, kad vertinimas pagal šį metodą yra itin patikimas.

Kad ekspertinės sistemos pateikiamas duomenų saugumo įvertinimas būtų lengvai suvokiamas nuspręsta gautus rezultatus grupuoti į kategorijas, atspindinčias duomenų saugumo lygį. Panašus grupavimas yra atliekamas saugumą vertinant pagal ISO 15504 standartą grupuojant proceso atributus (žiūr. 3 lent.). Nuspręsta, klasifikuoti saugumo lygį ne į keturias kategorijas kaip atliekama pagal ISO standartą, bet į penkias ir tokiu būdu pateikti klientui tikslesnį jo turimų duomenų apsaugos lygio įvertinimą.

Vartotojui atsakinėjant į ekspertinės sistemos užduodamus klausimus yra skaičiuojamas kiekvienos grėsmės galimos padaryti žalos koeficientas. Panašūs skaičiavimai atliekami išlaidų bei gaunamos naudos metode atliekant grėsmių indeksų apskaičiavimą. Daroma prielaida, kad skirtingų

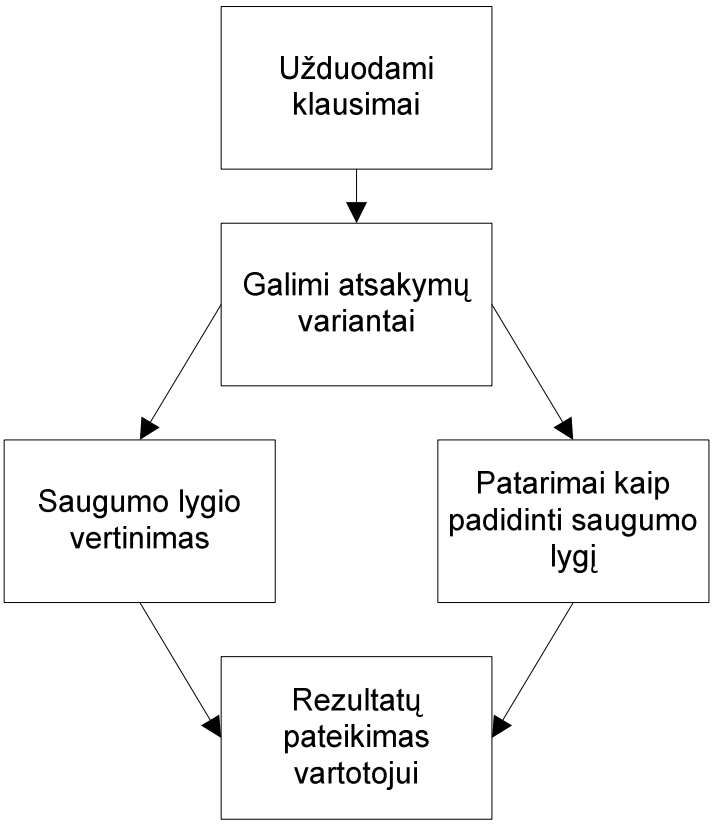
grėsmių yra skirtinga tikėtina žala kompiuteryje esančių duomenų saugumui ir dėl to grėsmės yra sugrupuojamos. Pasirinkta grėsmes grupuoti į devynias kategorijas (plačiau žiūr. 10 lent.).

Apibendrinimas. Ekspertinė sistema yra pranašesnė už duomenų bazę tuo, kad duomenų bazės tik iškviečia ir pateikia joje laikomus duomenis, o ekspertinė sistema analizuoja duomenis bei pateikia išvadas. Nuspręsta kurti ekspertinę sistemą, kuria galėtų naudotis net pradedantysis kompiuterio vartotojas. Sistema yra orientuota į mažai žinių apie duomenų saugumą turinčius žmones, nes darytina išvada, kad būtent jiems ekspertinės sistemos pateikiami patarimai ir rekomendacijos yra reikalingiausios.

2.2. Ekspertinės sistemos veikimo principas

Sukurta ekspertinė sistema remiasi ISO 15504 standarte naudota skaičiavimo metodika bei išlaidų ir gaunamos naudos metode naudotais skaičiavimais. Jei į visus ekspertinės sistemos užduodamus klausimus vartotojas atsako taip, kad grėsmių galima įtaka jo duomenų saugumui yra maksimali – ekspertinės sistemos pateikiamas saugumo lygis vis tiek negali būti žemesnis kaip nulis procentų. Ekspertinės sistemos pateikiamas duomenų apsaugos priemonių patikimumo lygis svyruoja nuo 0 iki 99 %. (kai 99% yra aukščiausias įvertinimas 100 balų sistemoje, nes šimtaprocentinio sistemos patikimumo niekuomet nebūna).

Ekspertinės sistemos įvertinančios duomenų saugumo lygį veikimo principas yra pavaizduotas 3 paveikslėlyje. Vartotojui yra užduodami klausimai ir pateikiami galimi atsakymo variantai. Kiekvieną kartą vartotojui atsakant į klausimus ekspertinė sistema atlieka veiksmus, kurių vartotojas nemato, t.y. skaičiuoja dabartinį duomenų saugumo lygį bei kaupia patarimus, kaip padidinti duomenų saugumo lygį, kurie vartotojui yra pateikiami tik atsakius į visus sistemos užduodamus klausimus. Vartotojui pateikiant duomenų apsaugos priemonių saugumo lygio įvertinimas yra pateikiamas ne tik 100 proc. sistemoje, bet ir žodine išraiška (pvz. patikimumas yra patenkinamo, kritinio lygio ir pan.).



Šaltinis: sudaryta darbo autorės.

3 pav. Ekspertinės sistemos įvertinančios duomenų saugumo lygį veikimo principas

Prieš pradedant kurti ekspertinę sistemą yra labai svarbu žinoti, ne tiktai kokius rezultatus ji generuos, bet kas atsakinės į sistemos užduodamus klausimus. Vienaip klausimai būtų formuluojami, jei būtų pritaikyti atsakinėti tik kompiuterių priežiūros specialistams, kitaip klausimai yra formuluojami, kai į juos gali atsakyti kompiuterio vartotojai. Nutarta kurti ekspertinę sistemą į kurios klausimus galėtų atsakyti namų kompiuteriu besinaudojantys vartotojai neturintys daug patirties dirbant su kompiuteriu bei apsaugant kompiuteryje esančius duomenis, nes manoma, kad tai galėtų padėti padidinti saugumo lygį tuose kompiuteriuose, kurių savininkai skiria mažai dėmesio jų saugumo lygio užtikrinimui. Yra tikėtina, kad jei žmogus nustatys savo kompiuterio saugumo lygį ir gaus žemus saugumo rezultatus bei nemažai patarimų, kaip padidinti duomenų apsaugos lygį esantį kompiuteryje, yra tikėtina, kad jis įgyvendins bent dalį iš pateiktų patarimų.

Vartotojui yra labai svarbu, kad sistemos užduodami klausimai būtų lengvai suprantami, o atsakymai nebūtų painūs bei gaunamas įvertinimas būtų suprantamas, o patarimai konkretūs. Stengiantis įgyvendinti šiuos uždavinius kuriant ekspertinę sistemą labai svarbu nenaudoti specifinių terminų, kurie būtų žinomi tik tam tikros specialybės atstovams.

Kad atsakinėjimas į klausimus būtų paprastas ir vartotojui nereikėtų galvoti, kada galima pasirinkti kelis atsakymo variantus, kada užtenka pasirinkti tik vieną nuspręsta sukurti ekspertinę sistemą, kurioje visuomet reikėtų žymėti tik vieną atsakymo variantą, dėl to dauguma klausimų yra

pradedami klausiamuoju žodeliu „ar“, tai iš kart signalizuoja, kad klausimas yra uždaras ir reikalauja ne išsamaus paaiškinimo, o konkretaus atsakymo.

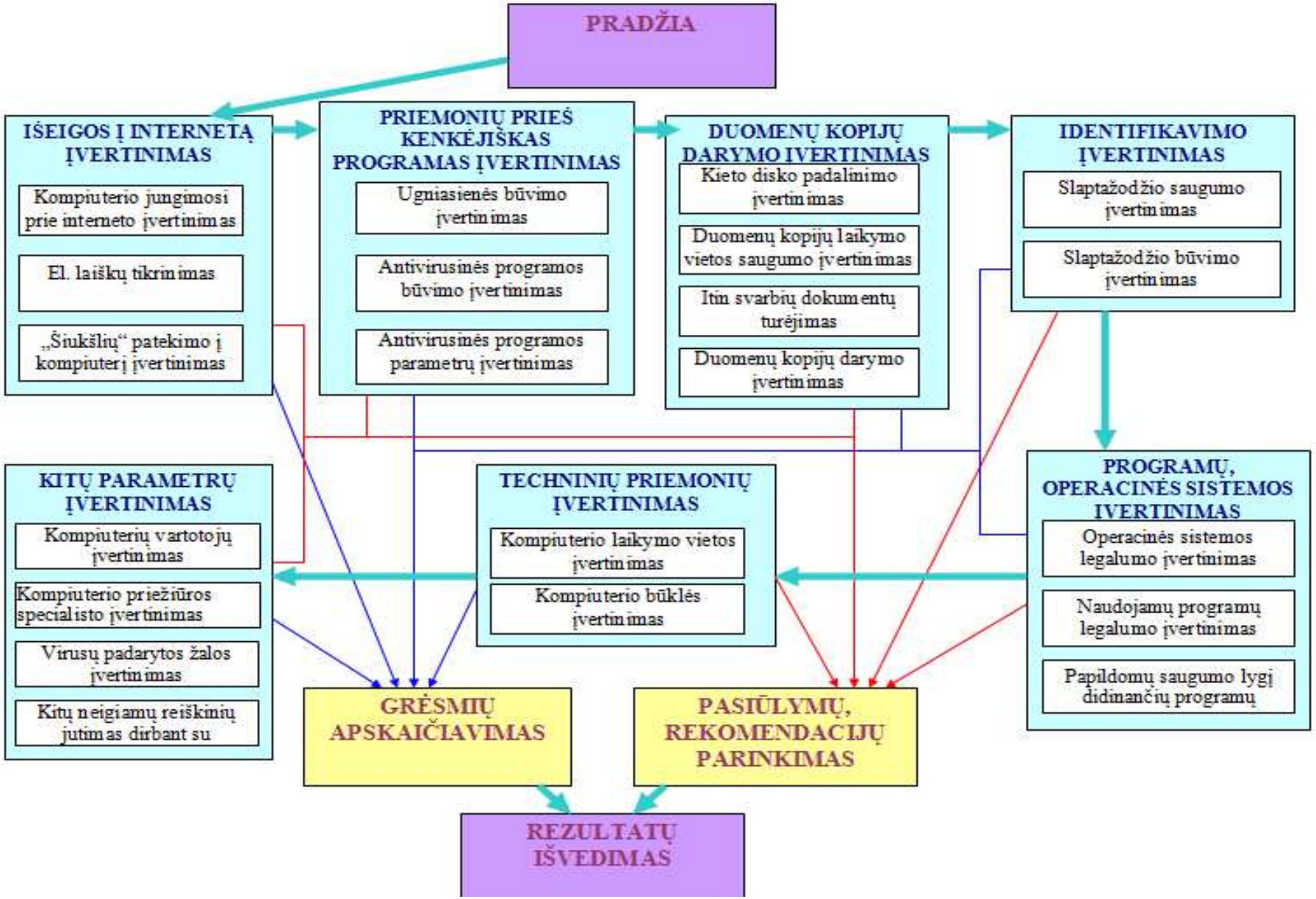
Vartotojo patogumui atsakinėjant į ekspertinės sistemos užduodamus klausimus visuomet yra suteikiama galimybė nustoti atsakinėt į juos, tokiu atveju vartotojui yra pateikiamas pranešimas, kad duomenų saugumo lygio nepavyko įvertinti dėl to, kad nebuvo atsakyta į visus reikiamus klausimus.

Duomenų saugumo lygio vertinimas remiantis dviejų metodikų skaičiavimo pagrindais, pateikiami patarimai vartotojui (ko nedaro nei viena saugumo lygį vertinanti metodika) bei galimybė į nieką nesikreipti, o tiesiog būnant savo namuose įvertinti duomenų saugumo lygį – tai yra šios ekspertinės sistemos privalumai.

Ekspertinės sistemos struktūrinė schema pateikta 4 pav. Ekspertinės sistemos užduodamus klausimus galima sugrupuoti į septynias grupes:

- išeigos į internetą įvertinimas,
- priemonių prieš kenkėjiškas programas įvertinimas,
- duomenų kopijų darymo įvertinimas,
- identifikavimo įvertinimas,
- programų, operacinės sistemos įvertinimas,
- techninių įvertinimas,
- kitų parametrų įvertinimas.

Užduodamų klausimų eiliškumas priklauso nuo vartotojų atsakymų. Atsakinėjant į klausimus (žydros sp. rodyklės) programa skaičiuoja grėsmes galimą padaryti žalą kompiuterinei sistemai (mėlynos sp. rodyklės) bei yra parenkami patarimai (raudonos sp. rodyklės), kurie išvedami į ekraną vartotojui baigus atsakinėt į klausimus.



Šaltinis: sudaryta darbo autorės.

4 pav. Ekspertinės sistemos struktūrinė schema

Apibendrinimas. Ekspertinės sistemos įvertinančios duomenų saugumo lygį veikimo principas yra paremtas tuo, kad vartotojui yra užduodami klausimai ir pateikiami galimi atsakymo variantai. Kiekvieną kartą vartotojui atsakant į klausimus ekspertinė sistema atlieka veiksmus, kurių vartotojas nemato, t.y. skaičiuoja dabartinį duomenų saugumo lygį bei kaupia patarimus, kaip padidinti duomenų saugumo lygį, kurie vartotojui yra pateikiami tik atsakius į visus sistemos užduodamus klausimus.

2.3. Duomenų apsaugos priemonių automatizuoto įvertinimo išvados

Šiuo metu naudojamos metodikos, skirtos duomenų saugumo lygio nustatymui, turi trūkumų: yra neišvengiama subjektyvumo vertinant saugumo lygį remiantis jomis, sugaištama nemažai laiko norint išsiaiškinti duomenų saugumo lygį bei išsiaiškinus kompiuterinės sistemos saugumo lygį yra nežinoma kokių konkrečių veiksmų reikėtų imtis, kad saugumas būtų aukštesnio lygio. Dažniausiai klientui yra suteikiama tik informacija, ką daryti, kad patikimumo/saugumo lygis pereitų į kitą aukštesnį etapą. Šias problemas padėtų išspręsti ekspertinė saugumą vertinanti programa.

Ekspertinė sistema pateikia išvadas iš jai pateiktų duomenų arba išsprendžia tam tikrus uždavinius. Ekspertinė sistema visuomet yra kompiuterinė programa. Ši sistema yra pranašesnė už duomenų bazę tuo, kad duomenų bazės tik iškviečia ir pateikia joje laikomus duomenis, o ekspertinė sistema analizuoja duomenis bei pateikia išvadas.

Nuspręsta kurti ekspertinę sistemą, kuria galėtų naudotis net pradedantysis kompiuterio vartotojas. Sistema yra orientuota į mažai žinių apie duomenų saugumą turinčius žmones, nes darytina išvada, kad būtent jiems ekspertinės sistemos pateikiami patarimai ir rekomendacijos yra reikalingiausios.

Ekspertinės sistemos įvertinančios duomenų saugumo lygį veikimo principas yra paremtas tuo, kad vartotojui yra užduodami klausimai ir pateikiami galimi atsakymo variantai. Kiekvieną kartą vartotojui atsakant į klausimus ekspertinė sistema atlieka veiksmus, kurių vartotojas nemato, t.y. skaičiuoja dabartinį duomenų saugumo lygį bei kaupia patarimus, kaip padidinti duomenų saugumo lygį, kurie vartotojui yra pateikiami tik atsakius į visus sistemos užduodamus klausimus.

3. DUOMENŲ APSAUGOS PRIEMONIŲ EKSPERTINĖ SISTEMA

Šio tyrimo tikslas – įvertinti duomenų saugos lygį bei patarti vartotojui, kokių veiksmų jis turėtų imtis norėdamas padidinti duomenų esančių kompiuteryje saugos lygį. Tam, kad būtų įvertinta duomenų sauga buvo sukurta bei ištestuota ekspertinė sistema, įvertinti sukurtos sistemos rezultatai.

3.1. Tyrimo duomenys

Išanalizavus metodikas kaip galima įvertinti duomenų saugumo lygį buvo nutarta kurti ekspertinę sistemą, kuri kompiuterinę sistemą vertintų šiais aspektais:

- slaptažodžio buvimas, jo saugumas,
- antivirusinės programos buvimas, jos saugumas,
- operacinės sistemos legalumas,
- naudojamų programų legalumas,
- „šiukšlių“ patekimo į kompiuterį rizikos įvertinimas,
- ugniasienės buvimas (jei kompiuteris turi išeigą į internetą),
- kompiuterio laikomo vietos saugumas,
- vartotojų (-o) besinaudojančių (-io) kompiuteriu patikimumas,
- papildomų laikmenų prijungimo prie kompiuterio dažnumas,
- duomenų kopijų darymas bei jų laikymo vietos patikimumas,
- itin svarbių duomenų turėjimas,
- diegimas į kompiuterį abejotinos vertės programų,
- kompiuterio būklės įvertinimas,
- saugumo lygį kompiuteryje didinančių programų naudojimas,
- papildomų neigiamų reiškinių jutimas dirbant su kompiuteriu.

Vertinant kompiuterinę sistemą yra atsižvelgiama ne tik į kompiuteryje įdiegtas programas, jų legalumą, bet ir į vartotojo atliekamus veiksmus, nes net turint visą reikiamą programinę įrangą, bet netinkamai su ja elgiantis yra sumažinamas kompiuteryje esančių duomenų saugumo lygis. Taip pat galima paminėti kitą atvejį: jei kompiuteryje yra įdiegta tinkama programinė įranga, vartotojas elgiasi vadovaudamasis visomis saugumo taisyklėmis, bet kompiuteris yra laikomas nepatikimoje vietoje (yra didelė tikimybė jį pavogti, užlieti vandeniu ar pan.) – tokiu atveju duomenų esančių kompiuteryje saugumo taip pat negalima įvertinti aukščiausiais balais.

Apibendrinimas. Vertinant duomenų apsaugos priemones, pasirinkta kompiuterinę sistemą vertinti šiais aspektais: slaptažodžio buvimas (jo saugumas), antivirusinės programos buvimas (jos saugumas), operacinės sistemos, naudojamų programų legalumas, „šiukšlių“ patekimo į kompiuterį rizikos įvertinimas, ugniasienės buvimas (jei kompiuteris turi išeigą į internetą), vartotojų (-o) besinaudojančių (-io) kompiuteriu patikimumas ir t.t. Vertinant kompiuterinę sistemą yra atsižvelgiama ne tik į kompiuteryje įdiegtas programas, jų legalumą, bet ir į vartotojo atliekamus veiksmus.

3.2. Tyrimo eigos aprašymas

Duomenų saugos priemonių saugumo lygio nustatymo eiga yra pavaizduota 5 paveikslėlyje. Grėsmė - tai pavojus tykantis duomenų esančių kompiuteryje. Grėsmių identifikavimas aprašytas 3.1. skyriuje. Sekantis ne ką mažiau svarbus žingsnis – yra svorių parinkimas nustatytoms grėsmėms. Svoris – tai koeficientas, nustatantis grėsmės galimą padaryti žalą duomenų saugumui. Grėsmių svoriai yra aprašyti 10 lentelėje.

Žinant duomenų saugumui kylančias grėsmes bei jų galimą padaryti žalą reikia atsižvelgti, kad ta pati grėsmė skirtingose situacijose gali būti skirtingai žalinga. Niekas nepaneigs, kad virusų patekimas yra grėsmingas procesas kompiuteryje saugomų duomenų saugumui, tačiau vertinant duomenų apsaugos lygį skirtingai būtų vertinamas virusas, kuris sutrikdė įprastą kompiuterio vartotojo dienotvarkę (pvz. duomenys buvo išgadinti, jų nebuvo galima pasiekti ir pan.) ar kurio būvimas kompiuteryje nepadarė jokios žalos ir buvo laiku pašalintas. Toliau analizuojant virusų būvimo kompiuteryje žalą galima pastebėti, kad duomenų saugumas bus taip pat skirtingai vertinamas, jei virusų padaryta neigiama įtaka yra juntama kiekvieną savaitę ir jei ji buvo juntama vieną kart per pastarąjį pusmetį. Grėsmių detalizavimas yra aprašytas 10 lentelėje.

Turint apibrėžtas, detalizuotas grėsmes bei žinant jų svorius reikėjo suformuoti klausimus, kurie padėtų nustatyti duomenų saugos lygį. Sugalvojus klausimus bei galimus atsakymus reikėjo sudaryti klausimų pateikimo eiliškumą, pvz. atsakius į klausimą teigiamai, kad kompiuteryje yra interneto ryšys iš karto pateikiami klausimai apie ugniasienės būvimą kompiuteryje, naudojimąsi elektroniniu paštu bei nežinomų siuntėjų siunčiamų laiškų atidarinėjimo dažnumą ir t.t. Šių klausimų nepateikinėjama vartotojui, kuris atsakė, kad išeigos į internetą nėra jo naudojamame kompiuteryje. Klausimai ir jų eiliškumas bei galimi atsakymai pateikti 11 lentelėje.

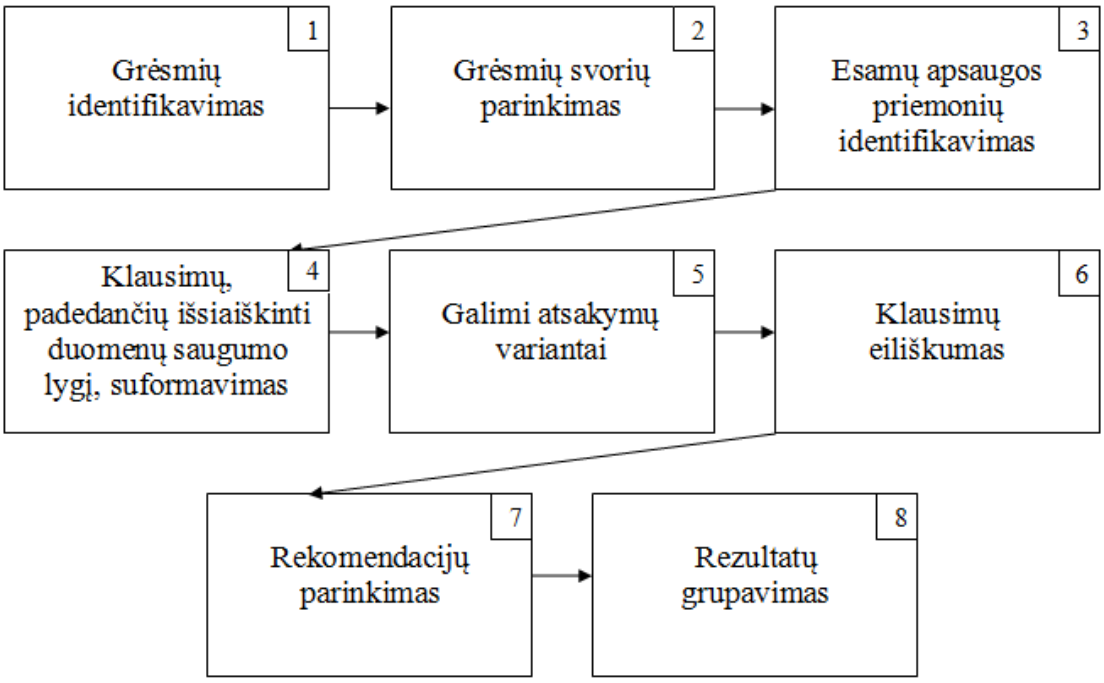
Prieš realizuojant programą reikėjo apsispręsti, kaip pateikti duomenų saugumo įvertinimo rezultatą klientui, kad gauti rezultatai būtų aiškūs ir suprantami. Nuspręsta rezultatus pavaizduoti spalviškai, raudona spalva, kadangi asocijuojasi su pavojumi ir grėsme- ji pasirinkta rodyti rezultatams, kurie atskindi žemą duomenų saugumo lygį, žalia spalva atspindi auštą patikimumo

lygį ir vidutinio saugumo duomenų atvaizdavimui pasirinkta geltona spalva. Rezultatai pateikiami ne tik spalviškai, bet ir įvardinant procentais duomenų saugumo lygį (žiūr. 12 lent.).

Žinant, kokius klausimus ir kada pateikti, kaip vertinti galimus atsakymus ir kaip pateikti gautus rezultatus buvo realizuota duomenų saugumo priemones įvertinanti programa. Duomenų saugumo lygis yra vertinamas šimto balų sistemoje (kai 99% yra pats didžiausias įvertinimas, nes 100% įvertinimo nebūna). Yra ne tik pateikiamas duomenų saugumo lygio įvertinimas, bet ir patarimai, kokių veiksmų reikėtų imtis norint padidinti duomenų saugumo lygį. Programos pateikiami klausimai matomi pirmame priede, o galimi skirtingi rezultatai vertinant duomenų saugumo lygį pateikti 7 - 11 paveikslėliuose.

Projektuojant ekspertinę sistemą yra atsižvelgiama į tai, kad sistema turi būti pritaikyta namų vartotojui, kuris neturi daug žinių apie duomenų esančių kompiuteryje saugumo lygio užtikrinimą bei kuris naudojasi Windows operacine sistema.

Vartotojas atsakinėdamas į ekspertinės sistemos klausimus nemato, kaip programa vertina konkretų jo atsakymą (tai nėra rodoma, nes jei į ekspertinės sistemos klausimus atsakinėtų kompiuterį prižiūrintis asmuo ir programos pateikiamą rezultatą turėtų kažkam pristatyti – jis būtų suinteresuotas gauti kuo aukštesnius rezultatus ir matydamas kaip programa vertina jo atsakymus, kiltų noras atsakyti ne visuomet teisybę į pateikiamus klausimus), nes ekspertinė sistema vartotojui pateikia tik galutinį duomenų apsaugos lygio įvertinimą. Norint ištestuoti ekspertinės sistemos veikimą buvo įkeltas papildomas laukelis į programą ir atsakinėjant į sistemos klausimus buvo galima matyti kaip kinta duomenų saugumo lygio įvertinimas (žiūr. 2 priedą).



Šaltinis: sudaryta darbo autorės.

5 pav. Duomenų apsaugos priemonių rinkinio įvertinimo etapai

Pasirinkti kriterijai, kuriais ruošiamasi įvertinti duomenų saugą, buvo patikslinti bei jiems priskirti svoriai. Tarkim analizuojant duomenų kopijų darymo dažnumą yra svarbu žinoti ne tik kaip dažnai jos yra daromos, bet taip pat svarbu žinoti ar kompiuteryje yra saugomi duomenys, kurių išgadinimas galėtų sukelti rimtų materialinių ar moralinių problemų. Svoriams yra suteikiamos nuo 8 iki 0,5 vertės. Aštuonetu yra įvertintos didžiausią grėsmę kompiuterinei saugai keliančios grėsmės, o puse balo vertinamos mažiausiai pavojingos grėsmės (žiūr. 10 lent.).

Prie didžiausią pavojų keliančių grėsmių (vertinamomis didžiausiu 8 balų svoriui) priskiriamos šios grėsmės: antivirusinės programos nebuvimas, kompiuterio laikymo vietos nesaugumas, virusų padarytos grėsmės padarytos neigiamos įtakos jautimas kiekvieną savaitę, bei kasdieninis susidūrimas su nelegalios operacinės sistemos netinkamu veikimu. Šios grėsmės yra priskiriamos prie pačių pavojingiausių, nes yra manoma, kad duomenys yra patys nesaugiausi kompiuteryje ir galima grėsmė jų saugumui yra labai tikėtina.

Į žemesnę kategoriją patenka šios grėsmės: kompiuteryje yra laikomi itin svarbūs duomenys, bet duomenų kopijos nėra daromos bei kompiuterio kietojo disko nepadalinimas. Kietojo disko padalinimas bent į dvi dalis, kurioje vienoje iš jų būtų saugomos programos, o kitame duomenys leistų kompiuterio vartotojui saugiau jaustis net virusui patekus į kompiuterį, tad jei nėra dirbama remiantis šiuo saugumo principu tai yra įvardijama kaip stipri grėsmė duomenų saugumo lygiui.

Didelę grėsmę duomenų saugumui kelia ir šios grėsmės: ugniasienės nebūvimas, kai kompiuteris turi išeigą į internetą bei dažnas abejotinos vertės programų diegimas. Šios grėsmės vertinamos 6 balais (iš 8 galimų). Norint būti saugiam naudojantis internetu reikia naudoti ne tik patikimą, savaime atsinaujinančią antivirusinę programą bet taip pat naudoti ugniasienę. Jei kompiuterio vartotojas dažnai diegia į savo kompiuterį programas apie kurių veikimą jis neturi pakankamai žinių yra nemaža tikimybė, kad jis atsisiųs tokiu būdu ir programų su virusais.

Prie vidutinė grėsmę duomenų saugumui sukeliančių grėsmių yra priskiriamos šios grėsmės: slaptažodžio nebūvimas pradedant darbą kompiuteriu, duomenų kopijų nedarymas, nelegalios operacinės sistemos arba virusų sutrikdymas kasdieninės vartotojo veiklos. Jei virusų padaryta žala arba nelegali operacinė sistema veikia taip, kad vartotojas negali atlikti savo įprastų kasdieninių darbų – tai tokios grėsmės negali būti vertinamos mažais svoriais, nes kelia rimtą pavojų duomenų saugumui.

Jei vartotojas turi antivirusinę programą, bet ji nėra automatiškai atsinaujinanti ir vartotojas pamiršta ją reguliariai atnaujinti arba kompiuterio laikymo vietos pakankamo saugumo nebūvimas, arba jei prie kompiuterio kasdien jungiamos išorinės informacijos laikmenos – visos šios grėsmės taip pat mažina kompiuterio duomenų saugumo lygį ir yra vertinama 4 balais. Išorinėse laikmenose,

ypač gaunamose iš nepatikimų šaltinių, yra didelė tikimybė aptikti virusą, tad ši grėsmė, kaip ir kitos ką tik išvardintos yra priskiriamos prie vidutinio pavojingumo, nes yra manoma, kad duomenys yra gana nesaugūs kompiuteryje ir yra nemaža tikimybė, kad jie gali būti išgadinti.

Trimis balais yra vertinamos šios grėsmės: kasdien yra atidarinėjami nežinomų siuntėjų siunčiami laiškai, kartais diegiamos abejotinos vertės programos, dažnai susiduriama su nelegalios operacinės sistemos netinkamu veikimu, nelegalių programų naudojimas, jei virusai buvo sutrikdę kompiuterio darbą, kai dažnai yra juntama neigiama virusų įtaka dirbant su kompiuteriu, kai itin svarbių dokumentų kopijos daromos rečiau nei vieną kartą į pusmetį ar kai dažnai yra prijungiamos prie kompiuterio papildomos informacijos laikmenos. Itin svarbių duomenų apsauga reikia itin atidžiai rūpintis, nes jų išgadinimas ir praradimas sukeltų didelių finansinių ar moralinių problemų, tad itin svarbių duomenų darymas rečiau nei kartą į pusmetį yra priskiriama prie grėsmių. Taip pat, jei vartotojas naudoja nelegalias programas – duomenys, esantys kompiuteryje nėra patikimai apsaugoti, nes programų siuntimas į savo kompiuterį, apie kurių veiklą nėra pakankamai žinoma, gali sutrikdyti kompiuterio darbą.

Jei kartais pamirštama atnaujinti antivirusinę programą ar itin svarbių dokumentų kopijos daromos vieną kartą į pusmetį, kompiuteriu naudojasi keli vartotojai, ar jei dažnai yra atidarinėjami nežinomų siuntėjų siunčiami laiškai, padarytos duomenų kopijos yra laikomos nesaugioje vietoje, ar jei duomenų kopijos daromos rečiau nei kartą į pusmetį – visos šios sąlygos taip pat mažina duomenų saugumo lygį ir yra įvertinama kaip dviejų balų grėsmė. Jei kompiuteriu naudojasi ne vienas vartotojas – grėsmė kylanti kompiuterio saugumui bus visuomet didesnė nei besinaudojant vienam vartotojui, net tokiu atveju jei kompiuteriu naudojasi ir iš pažiūros patikimas žmogus. Jei yra daromos duomenų kopijos – tai yra didinamas saugumo lygis esantis kompiuteryje, bet jei padarytos kopijos yra laikomos nesaugioje vietoje, pvz. duomenys yra kopijuojami į laikmeną, kuri yra laikoma tokioje vietoje, kur joje esančia informaciją gali lengvai naudotis pašaliniai asmenys ar ji gali būtų lengvai pavogta ar sugadinta – tokiu atveju duomenų saugumo lygis mažėja (Computer act!ve, 2009).

Vertinant grėsmes nėra apsieinama be subjektyvumo. Vartotojas atsakinėdamas į programos užduodamus klausimus gali vertinti savo jėgas, jei kompiuteriu naudojasi ne jis vienas- vartotojas gali įvertinti savo kolegų patikimumą. Kadangi šie atsakymai yra labai subjektyvus ir gali priklausyti nuo žmogaus nuotaikos bei jo požiūrio, tokiems atsakymams priskiriamas grėsmės svoris svyruojantis nuo 1 – 0,5.

10 lentelė

Grėsmės bei jų svoriai

Grėsmės svoris	Grėsmė	Komentaras
8	Antivirusinės programos nebuvimas	
	Kompiuteris laikomos nesaugioje vietoje	
	Kasdien susiduriama su nelegalios operacinės sistemos netinkamu veikimu	
	Kartą per savaitę yra juntama neigiama virusų įtaka dirbant su kompiuteriu	
7	Kompiuteryje yra itin svarbių dokumentų	Kai duomenų kopijos nėra daromos
	Kompiuteryje esantis kietasis diskas nėra padalintas	
6	Nėra įdiegtos ugniasienės	Kompiuteris turi prieigą prie interneto
	Dažnas abejotinos vertės programų diegimas	
5	Slaptažodžio nebūvimas pradedant darbą kompiuteriu	
	Duomenų kopijos nėra daromos	
	Nelegalios operacinės sistemos darbas trukdo kasdieninę veiklą	
	Virusai yra sutrikdę kasdieninę veiklą	
4	Pamirštama atnaujinti antivirusinę programą	Kai antivirusinė programa neatsinaujina savaime
	Kompiuteris laikomos nepakankamai saugioje vietoje	
	Kasdien yra prijungiamos prie kompiuterio papildomos informacijos laikmenos	
3	Kasdien yra atidarinėjami nežinomų siuntėjų siunčiami laiškai	
	Kartais diegiamos abejotinos vertės programos	
	Dažnai susiduriama su nelegalios operacinės sistemos netinkamu veikimu	
	Naudojamos nelegalios programos.	
	Virusai buvo sutrikdę kompiuterio darbą	
	Dažnai yra juntama neigiama virusų įtaka dirbant su kompiuteriu	
	Itin svarbių dokumentų kopijos daromos rečiau nei vieną kart į pusmetį	
	Dažnai yra prijungiamos prie kompiuterio papildomos informacijos laikmenos	
2	Kartais užmirštama atnaujinti antivirusinę programą	Kai antivirusinė programa neatsinaujina savaime
	Itin svarbių dokumentų kopijos daromos vieną kart į pusmetį	
	Kompiuteriu naudojasi keli vartotojai	
	Dažnai yra atidarinėjami nežinomų siuntėjų siunčiami laiškai	
	Padarytos duomenų kopijos yra laikomos nesaugioje vietoje	
	Duomenų kopijos daromos rečiau nei kartą į pusmetį	
1	Turima antivirusinė programa savaime neatsinaujina	
	Duomenų kopijos daromos vieną kartą į pusmetį	
	Kompiuteriu naudojasi keli vartotojai	
	Antrasis kompiuterio vartotojas neturi savo slaptažodžio bei prisijungimo vardo	
	Kompiuteryje yra itin svarbių dokumentų	

10 lentelės tęsinys

Grėsmės svoris	Grėsmė	Komentaras
	Kas mėnesį yra atidarinėjami nežinomų siuntėjų siunčiami laiškai	
	Naudojama operacinė programa nėra legali	
	Kartais susiduriama su nelegalios operacinės sistemos netinkamu veikimu	
	Vartotojas nemano, kad turi pakankamai žinių užtikrinti stabilų kompiuterio darbą	Kai vartotojas pats rūpinasi savo kompiuterio apsauga
	Kartais yra juntama neigiama virusų įtaka dirbant su kompiuteriu	
	Yra nepasitikima kitu kompiuterio vartotoju	Kai vartotojas neturi savo prisijungimo vardo bei slaptažodžio
	Kiti kompiuterio vartotojai neturi savo prisijungimo vardų bei slaptažodžių	Kompiuteriu naudojasi ne vienas vartotojas
	Yra nepasitikima kitais kompiuterio vartotojais	Kompiuteriu naudojasi ne vienas vartotojas
	Naudojamas slaptažodis yra sudarytas tik iš raidžių bei yra užrašytas	
	Vartotojo prisijungimo slaptažodis yra žinomas jo kolegomis bei jis yra sudarytas tik iš raidžių	Kompiuteriu naudojasi ne vienas vartotojas
	Kompiuteriu naudojasi du vartotojai	
	Yra manoma, kad žmogus (firma) besirūpinantis (-i) kompiuterio apsauga neturi pakankamai kompetencijos	Kompiuterio apsauga rūpinasi ne jo vartotojas
	Kartais yra prijungiamos prie kompiuterio papildomos informacijos laikmenos	
0,5	Kompiuteriu naudojasi du vartotojai	
	Kartais yra atidarinėjami nežinomų siuntėjų siunčiami laiškai	
	Retai yra juntama neigiama virusų įtaka dirbant su kompiuteriu	
	Itin svarbių dokumentų kopijos daromos vieną kart į mėnesį	
	Kai kurie kompiuterio vartotojai neturi savo prisijungimo vardo bei slaptažodžio	Kompiuteriu naudojasi ne vienas vartotojas
	Yra nepasitikima kai kuriais kompiuterio vartotojais	Kompiuteriu naudojasi ne vienas vartotojas
	Naudojamas slaptažodis yra užrašytas	
	Naudojamas slaptažodis yra sudarytas tik iš raidžių	

Šaltinis: sudaryta darbo autorės.

Turint apibrėžtas grėsmes kylančias duomenų saugumui esančių kompiuteryje 10 lentelėje aprašytos grėsmės buvo tikslinamos. Žodžiai „dažnai“, „kartais“, „retai“ ir pan. buvo keičiami į konkrečius išsireiškimus: kartą į pusmetį/ savaitę/ mėnesį ir pan. Turint sukonkretintas grėsmes buvo kuriama duomenų apsaugos priemones įvertinanti programa.

Programos užduodami klausimai, galimi atsakymai, saugumo įvertinimai bei programos patarimai/rekomendacijos yra pateikiami 11 lentelėje. Atsakius į programos pateikiamus klausimus - duomenų apsaugos priemonių sauga gali būti įvertinta nuo 0 iki 100 balų. Laikoma, kad duomenys esantys kompiuteryje yra visiškai saugūs, kai sistema saugumą įvertina maksimaliu balu ir atvirkščiai, kai duomenų sauga yra pačio žemiausio lygio – tuomet duomenų apsaugos priemonių saugumas yra vertinamos 0%.

Projektuojant ekspertinę sistemą buvo pritaikyta skaičiavimo metodika, kad kol nei viena grėsmė duomenų saugai nėra nustatyta - kompiuterinių duomenų saugumas yra vertinamas aukščiausiais balais. Kiekviena naujai aptikta grėsmė mažina duomenų saugos priemonių patikimumą numatytu procentu (sutampančiu su grėsmės svoriu).

Vienu metu vertinat vartotojo atsakymus jam skirti tiek teigiamus balus (už užtikrinamą aukštą duomenų saugumo lygį tam tikroje situacijoje) bei skirti neigiamus balus (už neužtikrinamą duomenų saugumo lygį konkrečioje situacijoje) nėra prasminga, nes tokiu atveju nebūtų galima užtikrinti, kad vartotojo gautas įvertinimas iš ties yra 100 balų vertinimo sistemoje, nes kaip matyti 11 lentelėje, klausimai nėra visi pateikinėjami vienas po kito (priklausomai nuo vartotojo atsakymų, dalis klausimų gali būti praleista (pvz. klientas atsako, kad nenaudoja slaptažodžio jungiantis prie kompiuterio – tuomet ekspertinė sistema nebeklaus ar jo naudojamas slaptažodis yra saugus) ar užduoti papildomi klausimai, kurie yra užduodami tik specifinėse situacijose (pvz. vartotojas atsako, kad naudojasi nelegalia operacine sistema - tuomet yra klausiama ar nelegalios operacinės sistemos darbas yra sutrikdęs vartotojo kasdieninę veiklą ir pan.).

Ši ekspertinė sistema turi du vienodus klausimus, kuriuos užduoda savo vartotojui, bet duomenų saugos vertinimas atsakant į šios sistemos klausimus yra nevienodas. Paanalizuokime konkrečius atvejus. Sistema klausia vartotojo: „Ar turite savo kompiuteryje itin svarbių duomenų, kurių išgadinimas ar patekimas į pašalinių asmenų rankas sukeltų rimtų finansinių/ moralinių problemų?“ ir atsakymai į šį klausimą galimi skirtingi, nes jei vartotojas nedaro duomenų kopijų ir savo kompiuteryje turi itin svarbių duomenų saugumas vertinamas mažesniu balu nei tuo atveju jei vartotojas duomenų kopijas daro.

Kitas pavyzdys, kai sistema užduoda vartotojui klausimą: „Ar kompiuteriu naudojatės tiktai Jūs ar prie jo prieigą turi ir kiti (-as) vartotojai (-as)?“ galimi saugumo vertinimai yra taip pat skirtingi. Jei jungiantis prie kompiuterio nėra prašoma įvesti vartotojo vardo bei slaptažodžio – tokiu atveju duomenų saugumo lygis yra vertinamas mažesniu balu, nei esant šiai situacijai: kompiuteriu naudojasi keli vartotojai, bet kiekvienas turi savo prisijungimo vardą bei slaptažodį.

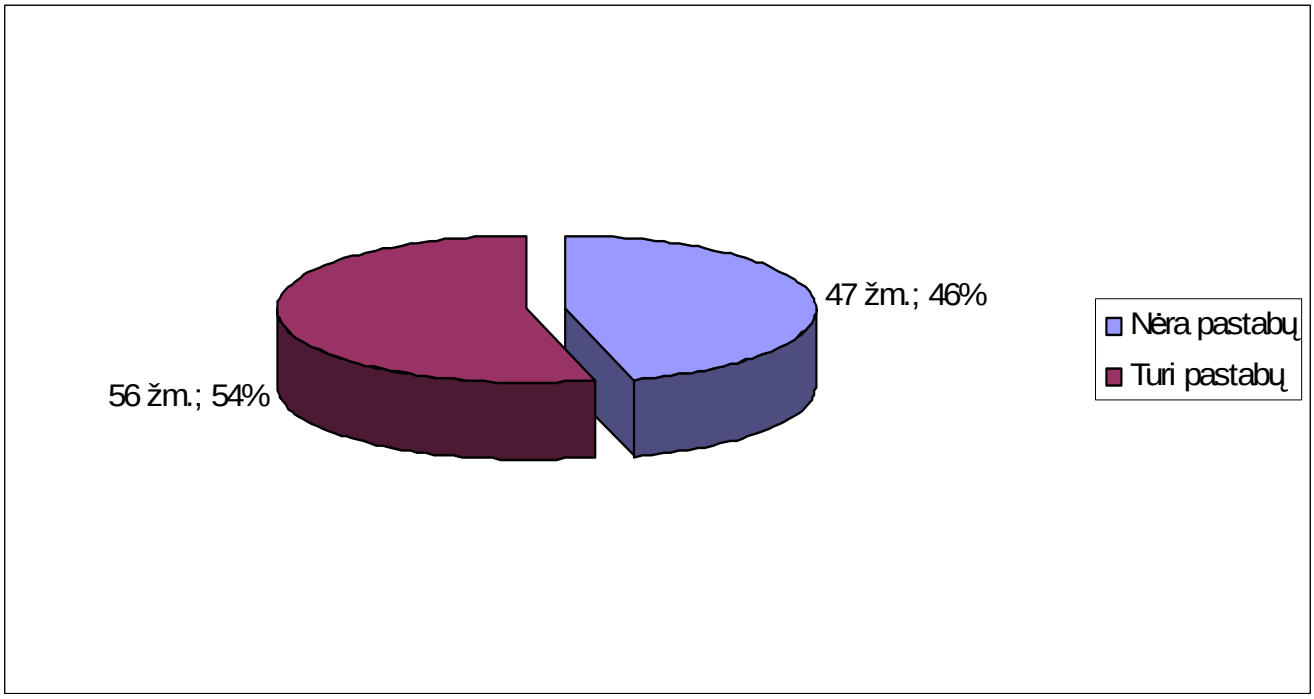
Analizuojant grėsmių pasirodymo dažnumą ne viename klausime yra pasirinktas laikotarpis: pastarasis pusmetis (analizuojant virusų padarytą žalą kompiuteryje, nežinomų siuntėjų atiderinėjamų laiškų dažnumą ir pan.). Šis laikotarpis yra pasirinktas, nes analizuojant trumpesnį laiko tarpą – vartotojo suvesti duomenys gali neatitikti realios situacijos, tarkim kompiuteryje kelis kartus per mėnesį pastebimi veiklos sutrikimai dėl naudojamos nelegalios operacinės sistemos, bet per pastarąją savaitę, jokių trikdžių nepastebėta. Analizuojant ilgesnį laikotarpį yra tikėtina, kad

vartotojas atsakinėdamas į programos klausimus, neprisimins kaip kompiuteris dirbo prieš metus laiko ar ankstesniu laikotarpiu. Be to yra didelė tikimybė, kad per ilgesnį laiko tarpą kompiuterine sistema pradėjo rūpintis kitas asmuo ar yra įdiegtos kitos programos ir duomenų sauga analizuojant laikotarpį prieš metus ir dabartinę situaciją gali ženkliai skirtis.

Remiantis 11 lentelėje išdėstyta medžiaga yra sukurta duomenų apsaugos priemones įvertinanti programa. Programa sukurta programavimo kalba C++. Sistemos pateikiami klausimai bei vartotojui rodomi informaciniai pranešimai yra pateikti 1 priede.

3.3. Apklausos rezultatai

Sukūrus programą ir ją ištestavus buvo nuspręsta įvertinti programos veikimą. Programa buvo duota testuoti žmonėms, kurie vertino savo turimo kompiuterio duomenų daugumo lygį. Buvo apklausti 103 respondentai (žiūr. 6 pav.). Norint, kad programa būtų išsamiai įvertinta programą vertino skirtingo amžiaus žmonės (apklaustųjų žmonių amžius nuo 17 iki 66 metų), skirtingų socialinių grupių žmonės (bedarbiai, moksleiviai, studentai, darbdaviai, samdomi darbuotojai, pensininkai), 47 apklaustieji neturėjo jokių komentarų programos veikimui (tai sudaro 45,6% iš visų apklaustųjų). Atsižvelgiant į likusių (54,4% iš visų apklaustųjų arba 56 žmonių) respondentų išsakytas pastabas programa buvo papildyta.



Šaltinis: sudaryta darbo autorės.

6 pav. Vartotojų apklausos rezultatai testuojant sistemą

6 paveikslėlyje preocentalia bei skaitine išraiška pavaizduoti sistemos testuotojų nuomonė apie sukurtą sistemą. Beveik pusė vartotojų apie programos užduodamus klausimus neturėjo pastabų, tai leidžia daryti prielaidą, kad arba programa patenkino jų lūkesčius, arba jie apie duomenų saugumo užtikrinimą turi labai mažai žinių (plačiau 3 priede). Esant pastarajam variantui reikia pasidžiaugti, kad būtent tokiems vartotojams ir yra kurta sistema (tiems, kas turi mažai žinių apie duomenų saugumo lygio užtikrinimą, esantį kompiuteryje, bet norintį, kad duomenys kompiuteryje būtų saugūs).

11 lentelėje pateikti ekspertinės sistemos užduodami klausimai, pateikiami patarimai, galimi atsakymų variantai bei grėsmei tenkantys balai:

11 lentelė

Ekspertinės sistemos užduodami klausimai bei pateikiami atsakymai bei grėsmės skaičiavimai

Klausimo Nr.	Klausimas	Galimi atsakymai	Įvertinimas	Patarimas, komentaras	Sekantis klausimas
1	Ar norite įvertinti duomenų, esančių Jūsų kompiuteryje, saugumo lygį?	Taip	-		2 klausimas
		Ne	-	Jūsų kompiuterinės sistemos saugumo nepavyko įvertinti, nes neatsakėte į visus klausimus	Pabaiga, kompiuterinės sistemos saugumo lygio nepavyko įvertinti
2	Ar Jūsų kompiuteris turi išeigą į internetą?	Taip	-		21 klausimas
		Ne	-		3 klausimas
3	Ar Jūsų kompiuteryje yra įdiegta antivirusinė programa?	Taip	-		4 klausimas
		Ne	- 6	Yra labai svarbu, kad kompiuteryje būtų įdiegta patikima antivirusinė sistema, kuri būtų reguliariai atnaujinama (pageidautina automatiškai)	42 klausimas
4	Ar Jūsų naudojama antivirusinė sistema automatiškai atnaujinama?	Taip	-		43 klausimas
		Ne	- 1		5 klausimas
5	Ar Jūs nepamirštate atnaujinti savo turimos antivirusinės sistemos nerečiau kaip 3 k. į sav.?	Nepamirštu	-		54 klausimas
		Kartais pamirštu	- 0,5	Rekomenduojame keisti Jūsų naudojamą antivirusinę programą į reguliariai atsinaujinančią, nes taip padidinsite savo kompiuterio saugumą)	54 klausimas
		Atnaujinu antivirusinę programą kasdien	-		54 klausimas
		Pamirštu	- 1	Rekomenduojame skubiai keisti Jūsų naudojamą antivirusinę programą į reguliariai atsinaujinančią, nes taip padidinsite savo kompiuterio saugumą)	43 klausimas

11 lentelės tęsinys

Klausimo Nr.	Klausimas	Galimi atsakymai	Įvertinimas	Patarimas, komentaras	Sekantis klausimas
6	Ar Jūsų kompiuteryje yra įdiegta ugniasienė (firewall)?	Taip	-		3 klausimas
		Ne	- 6	Rekomenduojame nedelsiant įsidiegti ugniasienę - tai padidintų Jūsų kompiuterio saugumą	3 klausimas
7	Ar prisijungiant prie kompiuterio reikia įvesti prisijungimo vardą, slaptažodį?	Taip	-		35 klausimas
		Ne	- 4	Norint padidinti duomenų saugumą kompiuteryje rekomenduojame, kad prisijungiant prie kompiuterio reikėtų suvesti vartotojo vardą bei slaptažodį.	38 klausimas
8	Ar kompiuteriu naudojatės tiktai Jūs ar prie jo prieigą turi ir kiti (-as) vartotojai (-as)?	Naudojuos tiktai aš	-		10 klausimas
		Turi prieigą kitas vartotojas	- 0,5		9 klausimas
		Turi prieigą kiti vartotojai	- 1		33 klausimas
9	Ar kitas vartotojas prisijungiant prie kompiuterio turi savo	Turi	-		36 klausimas
		Neturi	- 1	Siūlome vartotojui sukurti	32 klausimas
	prisijungimo vardą?			prisijungimo vardą bei slaptažodį, kad būtų užtikrintas kompiuterinių duomenų saugumas.	
10	Ar dirbdami su kompiuteriu darote duomenų kopijas?	Darau	-		11 klausimas
		Nedarau	- 5	Siūlome dirbant kompiuteriu reguliariai daryti duomenų kopijas.	31 klausimas
11	Ar turite savo kompiuteryje itin svarbių duomenų, kurių išgadinimas ar patekimas į pašalinių asmenų rankas sukeltų rimtų finansinių/ moralinių problemų?	Taip	- 1		30 klausimas
		Ne	-		12 klausimas
12	Kaip dažnai darote duomenų kopijas?	Kelis kartus per savaitę	-		13 klausimas
		Kartą per savaitę	-		13 klausimas
		Kartą į mėnesį	- 0,5		13 klausimas
		Kartą į pusmetį	- 1	Siūlome svarbių duomenų kopijas daryti reguliariai	13 klausimas
		Rečiau	- 2	Siūlome svarbių duomenų kopijas daryti reguliariai	13 klausimas

11 lentelės tęsinys

Klausimo Nr.	Klausimas	Galimi atsakymai	Įvertinimas	Patarimas, komentaras	Sekantis klausimas
13	Ar padarytas duomenų kopijas laikote saugioje, pašaliniams asmenims neprieinamoje vietoje?	Taip	-		14 klausimas
		Ne	- 2	Siūlome duomenų kopijas laikyti saugioje, niekam neprieinamoje vietoje	14 klausimas
14	Ar Jūsų kompiuteryje esantis kietasis diskas yra padalintas?	Taip	-		53 klausimas
		Ne	- 6	Yra labai svarbu kompiuteryje turėti bent su diskus, vieną - programų saugojimui, kitą - duomenų saugojimu.	53 klausimas
15	Ar Jūsų kompiuteris yra laikomas saugioje vietoje (t.y. šalia nėra sunkių daiktų, kurie galėtų krisdami pažeisti Jūsų kompiuterį, nėra didelės tikimybės, kad kompiuteris bus užlietas vandeniu, pavogtas ir pan.)?	Saugioje	-		16 klausimas
		Pakankamai saugioje	- 4	Siūlome padidinti kompiuterio saugumą pakeičiant jo darbo vietą arba sumažinant kompiuterio pavogimo tikimybę	16 klausimas
		Nesaugioje	- 8	Siūlome padidinti kompiuterio saugumą pakeičiant jo darbo vietą arba sumažinant kompiuterio pavogimo tikimybę	16 klausimas
16	Ar dažnai įsidiegiate į savo kompiuterį abejotinos vertės programas (programas apie kurių veikimą neturite pakankamai informacijos)?	Instaliuoju tik tas programas, kurių instaliaciniai failai pateikiami oficialiuose puslapiuose	-		17 klausimas
		Dažnai	- 6	Abejotinų/nežinomų programų diegimas mažina kompiuterio veiklos patikimumą. Patariame instaliuoti programas tik iš oficialių internetinių puslapių	17 klausimas
		Kartais	- 3	Abejotinų/nežinomų programų diegimas mažina kompiuterio veiklos patikimumą. Patariame	17 klausimas
				instaliuoti programas tik iš oficialių internetinių puslapių	
		Niekada	-		17 klausimas

11 lentelės tęsinys

Klausimo Nr.	Klausimas	Galimi atsakymai	Įvertinimas	Patarimas, komentaras	Sekantis klausimas
17	Ar Jūsų naudojama operacinė sistema yra legali?	Taip	-		20 klausimas
		Ne	- 1	Sistemos patikimumas mažėja naudojant nelegalią operacinę sistemą, nes jos veikimu negalime būti užtikrinti 100 proc.	18 klausimas
18	Ar susidūrėte su Jūsų turimos nelegalios operacinės programos netinkamu veikimu?	Taip	- 3		19 klausimas
		Ne	-		20 klausimas
19	Kaip dažnai per pastarąjį pusmetį susidūrėte su nelegalios operacinės programos netinkamu veikimu?	Kasdien	- 8	Siūlome keisti operacinę sistemą į legalią, nes dabartinė Jūsų turima sistema negali užtikrinti duomenų saugumo	24 klausimas
		Kelis kartus	- 3	Siūlome keisti operacinę sistemą į legalią, nes dabartinė Jūsų turima sistema negali užtikrinti duomenų saugumo	24 klausimas
		Vieną kartą	- 1		20 klausimas
		Nesusidūriau	-		20 klausimas
20	Ar visos Jūsų kompiuteryje esančios programos yra legalios?	Taip	-		45 klausimas
		Ne	- 3	Kompiuterinės sistemos patikimumas mažėja naudojant nelegalias programas, nes jų veikimu negalime būti užtikrinti 100 proc.	45 klausimas
21	Ar tikrinate el. paštą naudodamiesi savu kompiuteriu?	Taip	-		22 klausimas
		Ne	-		6 klausimas
22	Ar atidarinėjate nežinomų siuntėjų Jums el. paštu atsiųstus laiškus?	Taip	- 1		23 klausimas
		Kartais	- 0,5		23 klausimas
		Ne	-		6 klausimas
23	Kaip dažnai atidarinėjate nežinomų siuntėjų siunčiamus laiškus?	Kasdien	- 3	Siūlome keisti naudojamą el. pašto sistemą (pvz. į gmail, nes ši sistema gerai filtruoja spam'us). Niekuomet nepatariame atidarinėti nežinomų siuntėjų siunčiamų el. laiškų	6 klausimas

11 lentelės tęsinys

Klausimo Nr.	Klausimas	Galimi atsakymai	Įvertinimas	Patarimas, komentaras	Sekantis klausimas
		Vidutiniškai kartą į savaitę	- 2	Siūlome keisti naudojamą el. pašto sistemą (pvz. į gmail, nes ši sistema gerai filtruoja spam'us). Niekuomet nepatariame atidarinėti nežinomų siuntėjų siunčiamų el. laiškų	6 klausimas
		Vidutiniškai kartą į mėnesį	- 1	Niekuomet nepatariame atidarinėti nežinomų siuntėjų siunčiamų el. laiškų	6 klausimas
		Rečiau	-	Niekuomet nepatariame atidarinėti nežinomų siuntėjų siunčiamų el. laiškų	6 klausimas
24	Ar operacinės sistemos nestabilus darbas sutrikdė Jūsų kasdieninį darbą prie kompiuterio?	Taip	- 5	Siūlome nebeatidėlioti Jūsų turimos operacinės sistemos pakeitimo į legalią	20 klausimas
		Ne	-		20 klausimas
25	Ar Jūsų kompiuterio veiklą buvo sutrikdę virusai?	Taip	- 3		28 klausimas
		Ne	-		26 klausimas
26	Ar kompiuterio stabiliu veikimu rūpinatės Jūs pats (rūpinimasis stabiliu kompiuterio veikimu reiškia kompiuterio taisymo bei profilaktikos darbai)?	Taip	-		27 klausimas
		Ne	-		39 klausimas
27	Ar manote, kad turite pakankamai kompetencijos užtikrinti stabilų kompiuterio darbą?	Taip	-		7 klausimas
		Ne	- 1	Siūlome kompiuterio apsaugą patikėti patyrusiam specialistui arba pasikonsultuoti su patyrusiais specialistais, kaip užtikrinti kompiuteryje esančių duomenų apsaugą	7 klausimas
28	Kaip dažnai per pastarąjį pusmetį susidūrėte su virusų padaryta žala Jūsų kompiuteriui?	Pora kartų	- 1		29 klausimas
		Nesusidūriau	-		29 klausimas
		Vieną kartą	- 0,5		29 klausimas
		Kelis kartus	- 3	Rekomenduojame keisti Jūsų naudojamą antivirusinę sistemą	29 klausimas
		Vidutiniškai kartą į savaitę	- 8	Rekomenduojame nedelsiant keisti Jūsų naudojamą antivirusinę programą	29 klausimas
29	Ar virusų padaryta žala sutrikdė Jūsų kasdieninį darbą prie kompiuterio?	Taip	- 5		26 klausimas
		Ne	-		26 klausimas

11 lentelės tęsinys

Klausimo Nr.	Klausimas	Galimi atsakymai	Įvertinimas	Patarimas, komentaras	Sekantis klausimas
30	Kaip dažnai darote itin svarbių duomenų (kurių išgadinimas ar patekimas į pašalinių asmenų rankas sukeltų rimtų finansinių/ moralinių problemų) kopijas?	Kasdien	-		12 klausimas
		Kelis kartus per savaitę	-		12 klausimas
		Kartą per savaitę	-		12 klausimas
		Kartą į mėnesį	- 0,5	Siūlome itin svarbių dokumentų kopijas daryti reguliariai.	12 klausimas
		Kartą į pusmetį	- 2	Siūlome itin svarbių dokumentų kopijas daryti reguliariai	12 klausimas
		Rečiau	- 3	Siūlome itin svarbių dokumentų kopijas daryti reguliariai	12 klausimas
31	Ar turite savo kompiuteryje itin svarbių duomenų, kurių išgadinimas ar patekimas į pašalinių asmenų rankas sukeltų rimtų finansinių/ moralinių problemų?	Taip	- 7	Niekuomet nereikėtų pamiršti daryti itin svarbių dokumentų kopijų reguliariai.	14 klausimas
		Ne	-		14 klausimas
32	Ar pasitikite kitu vartotoju (ar tikite kad jis piktavališkais tikslais tikrai neišgadintų ir nekopijuotų Jūsų kompiuteryje turimų duomenų)?	Pasitikiu	-		10 klausimas
		Nepasitikiu	- 1	Naujas prisijungimo vardas bei slaptažodis jūsų kolegai turi būti sukurti neatidėliojant	10 klausimas
33	Ar kitiems vartotojams prisijungiant prie kompiuterio reikia įvesti prisijungimo vardą, slaptažodį?	Kiekvienas vartotojas turi savo prisijungimo vardą ir slaptažodį	-		37 klausimas
		Kai kurie vartotojai turi savo prisijungimo vardą ir slaptažodį	- 0,5	Siūlome visiems vartotojams sukurti prisijungimo vardus bei slaptažodžius, kad būtų užtikrintas duomenų saugumas	37 klausimas
		Neturi	- 1	Siūlome visiems vartotojams sukurti prisijungimo vardus bei slaptažodžius, kad būtų	34 klausimas

11 lentelės tęsinys

Klausimo Nr.	Klausimas	Galimi atsakymai	Įvertinimas	Patarimas, komentaras	Sekantis klausimas
				užtikrintas duomenų saugumas	
34	Ar pasitikite visais kitais vartotojais Jūsų kompiuterio naudotojais (ar tikite kad jie piktaviliškais tikslais tikrai neišgadintų ir nekopijuotų Jūsų turimų duomenų)?	Pasitikiu visais	-		10 klausimas
		Nepasitikiu	- 1	Siūlome visiems kompiuterio vartotojams nedelsiant sukurti prisijungimo vardus bei slaptažodžius, kad būtų užtikrintas duomenų saugumas	10 klausimas
		Pasitikiu kai kuriais vartotojais	- 0,5	Siūlome visiems kompiuterio vartotojams sukurti prisijungimo vardus bei slaptažodžius, kad būtų užtikrintas duomenų saugumas	10 klausimas
35	Ar Jūsų naudojamas slaptažodis yra saugus (t.y. jis sudarytas bent iš skaičių ir raidžių) ir jis nėra užrašytas kitiems prieinamoje vietoje?	Taip, aš laikausi šių slaptažodžio sudarymo bei saugojimo taisyklių	-		46 klausimas
		Esu užsirašęs slaptažodį, kad jo nepamirščiau	- 0,5	Rekomenduojame savo naudojamo slaptažodžio niekur neužsirašinėti, o jei tai darote, pasirūpinti, kad niekas neturėtų prieigos prie Jūsų užrašų	46 klausimas
		Mano slaptažodis sudarytas tik iš raidžių	- 0,5	Rekomenduojame pasikeisti savo naudojamą slaptažodį į tokį, kurį sudarytų tiek raidės, tiek skaičiai (siūloma naudoti ir skyrybos ženklus, jei reikalingas aukštesnio lygio duomenų saugumas)	46 klausimas

11 lentelės tęsinys

Klausimo Nr.	Klausimas	Galimi atsakymai	Įvertinimas	Patarimas, komentaras	Sekantis klausimas
		Mano slaptažodis sudarytas tik iš raidžių bei jį esu užsirašęs	- 1	Rekomenduojame pasikeisti savo naudojamą slaptažodį į tokį, kurį sudarytų tiek raidės, tiek skaičiai (siūloma naudoti ir skyrybos ženklus, jei reikalingas aukštesnio lygio duomenų saugumas), taip pat rekomenduojame savo naudojamo slaptažodžio niekur neužsirašinėti, o jei tai darote, pasirūpinti, kad niekas neturėtų prieigos prie Jūsų užrašų	46 klausimas
36	Ar kito vartotojo naudojamas slaptažodis yra saugus (t.y. jis sudarytas bent iš skaičių ir raidžių) ir jis nėra užrašytas kitiems prieinamoje vietoje?	Neturiu informacijos	-	Rekomenduojame naudoti slaptažodžius, sudarytus tiek iš raidžių, tiek iš skaičių (siūloma naudoti ir skyrybos ženklus jei reikalingas aukštesnio lygio duomenų saugumas.	10 klausimas
		Aš žinau jo prisijungimo vardą bei slaptažodį ir slaptažodis yra sudarytas tik iš raidžių	- 1	Siūlome, kad slaptažodį jungiantis prie kompiuterio žinotų tik vartotojas. Taip pat rekomenduojame naudoti slaptažodį, sudarytą tiek iš raidžių, tiek iš skaičių (siūloma naudoti ir skyrybos ženklus, jei reikalingas aukštesnio lygio duomenų saugumas).	10 klausimas
		Aš žinau jo prisijungimo vardą bei slaptažodį ir slaptažodis yra tinkamai sudarytas	-	Siūlome, kad slaptažodį jungiantis prie kompiuterio žinotų tik vartotojas.	10 klausimas

11 lentelės tęsinys

Klausimo Nr.	Klausimas	Galimi atsakymai	Įvertinimas	Patarimas, komentaras	Sekantis klausimas
37	Ar kitų vartotojų naudojami slaptažodžiai yra saugus (t.y. jie sudaryti bent iš skaičių ir raidžių) ir jie nėra užrašyt kitiems prieinamoje vietoje?	Naudojami slaptažodžiai nėra saugūs	- 1	Siūlome, kad slaptažodį jungiantis prie kompiuterio žinotų tik jo vartotojas. Taip pat rekomenduojame naudoti slaptažodžius, sudarytus tiek iš raidžių, tiek iš skaičių (siūloma naudoti ir skyrybos ženklus, jei reikalingas aukštesnio lygio duomenų saugumas)	34 klausimas
		Neturiu informacijos	-	Rekomenduojame naudoti slaptažodžius, sudarytus tiek iš raidžių, tiek iš skaičių (siūloma naudoti ir skyrybos ženklus, jei reikalingas aukštesnio lygio duomenų saugumas	34 klausimas
		Naudojami slaptažodžiai yra saugūs	-	Siūlome, kad slaptažodį jungiantis prie kompiuterio žinotų tik jo vartotojas.	10 klausimas
38	Ar kompiuteriu naudojatės tiktai Jūs ar prie jo prieigą turi ir kiti (-as) vartotojai (-as)?	Naudojuosi tiktai aš	-		10 klausimas
		Turi prieigą kitas vartotojas	- 1	Kiekvienas vartotojas pradėdamas darbą su kompiuteriu turi suvesti savo prisijungimo vardą ir slaptažodį- tai padidintų duomenų esančių kompiuteryje saugumą.	32 klausimas
		Turi prieigą kiti vartotojai	- 2	Kiekvienas vartotojas pradėdamas darbą su kompiuteriu turi suvesti savo prisijungimo vardą ir slaptažodį- tai padidintų duomenų esančių kompiuteryje saugumą.	34 klausimas
39	Kas rūpinasi jūsų kompiuterio saugumu?	Specialistas	-		40 klausimas
		Speciali firma	-		41 klausimas
		Draugas	-		40 klausimas
40	Ar manote, kad žmogus besirūpinantis	Taip	-		7 klausimas

11 lentelės tęsinys

Klausimo Nr.	Klausimas	Galimi atsakymai	Įvertinimas	Patarimas, komentaras	Sekantis klausimas
	Jūsų kompiuterio saugumu turi pakankamai kompetencijos užtikrinti stabilų kompiuterio darbą?	Ne	- 1	Patariame susirasti patikimesnį žmogų (firmą) ar patiems išsamiau pasidomėti Jūsų kompiuterio apsauga	7 klausimas
41	Ar manote, kad firma besirūpinanti Jūsų kompiuterio saugumu turi pakankamai kompetencijos užtikrinti stabilų kompiuterio darbą?	Taip	-		7 klausimas
		Ne	- 1	Patariame susirasti patikimesnį žmogų (firmą) ar patiems išsamiau pasidomėti Jūsų kompiuterio apsauga	7 klausimas
42	Ar dažnai prie kompiuterio prijungiate išorinės laikmenas (CD, DVD, USB ir t.t.)?	Kasdien	- 3	Išorinių laikmenų prijungimas prie kompiuterio mažina kompiuterio patikimumą, reikėtų pasirūpinti, kad antivirusinė programa automatiškai tikrintų kiekvieną informacijos laikmeną, prijungiamą prie kompiuterio	25 klausimas
		Niekada	-		25 klausimas
		Kartais	- 1	Išorinių laikmenų prijungimas prie kompiuterio mažina kompiuterio patikimumą, reikėtų pasirūpinti, kad antivirusinė programa automatiškai tikrintų kiekvieną informacijos laikmeną, prijungiamą prie kompiuterio	25 klausimas
		Dažnai	- 2	Išorinių laikmenų prijungimas prie kompiuterio mažina kompiuterio patikimumą, reikėtų pasirūpinti, kad antivirusinė programa automatiškai tikrintų kiekvieną informacijos laikmeną, prijungiamą prie kompiuterio	25 klausimas
43	Ar Jūsų naudojama antivirusinė programa yra paminėta šiame sąraše: Kaspersky, Norton, Extendia, Panda, AVG, ClamWin, McAfee ?	Taip	-		44 klausimas
		Ne	**0,5**	Patariame naudoti Antivirusinę sistemą, kuri yra patikima, pvz. Kaspersky, Norton, Extendia, Panda, AVG, ClamWin, McAfee.	44 klausimas

11 lentelės tęsinys

Klausimo Nr.	Klausimas	Galimi atsakymai	Įvertinimas	Patarimas, komentaras	Sekantis klausimas
44	Ar naudojates naujausia antivirusinės programos versija?	Taip	**-**		42 klausimas
		Ne	**0,5**		42 klausimas
45	Kada buvo įsigytas kompiuteris ar kada paskutinį kartą buvo atnaujinta Jūsų kompiuterio techninė įranga?	Šiais metais	**-**		48 klausimas
		Praeitais metais	**-**		48 klausimas
		Prieš kelerius metus	**0,5**	Nepamirškite, kad kompiuterinę techniką reikia tinkamai prižiūrėti bei prireikus atnaujinti.	48 klausimas
		Seniau nei prieš 10 metų	**1**	Nepamirškite, kad kompiuterinę techniką reikia tinkamai prižiūrėti bei prireikus atnaujinti.	48 klausimas
46	Ar naudojamo slaptažodžio saugumą nustatėte su specialia programa (pvz.: Redhad, Magic Key, The Block ar kt.)?	Taip	**-**		47 klausimas
		Ne	**-**	Norėdami įsitikinti, kad Jūsų slaptažodis yra iš ties patikimas, jo saugumą galite patikrinti su specialia programa (pvz.: Redhad, Magic Key, The Block ar kt.)?	51 klausimas
47	Kaip buvo įvertintas Jūsų naudojamas slaptažodis su specialia programa (pvz. Redhad, Magic Key, The Block ar kt.)?	Slaptažodis įvertintas kaip itin saugus	**-**		51 klausimas
		Slaptažodis įvertintas kaip saugus	**-**		51 klausimas
		Slaptažodis įvertintas kaip pakankamai saugus	**-**		51 klausimas
		Slaptažodis įvertintas kaip nepakankamai saugus	**0,5**	Rekomenduojame Jums pasikeiti slaptažodį į saugesnį.	51 klausimas
48	Ar jaučiate papildomų neigiamų reiškinių dirbat su kompiuteriu (pvz.: kompiuterį kartais tenka perkrauti norint toliau dirbti su juo, kartais kompiuteris bedirbant su juo persikrauna, išsijungia ir pan.)?	Taip	**1**		49 klausimas
		Kartais	**0,5**		49 klausimas
		Ne	**-**		50 klausimas

11 lentelės tęsinys

Klausimo Nr.	Klausimas	Galimi atsakymai	Įvertinimas	Patarimas, komentaras	Sekantis klausimas
49	Kaip dažnai jaučiate papildomus neigiamus reiškinius dirbant su kompiuteriu?	Kasdien	**3**	Patariame Jums skubiai šalinti neigiamus reiškinius juntamus dirbant su kompiuteriu, jei to negalite atlikti patys – kreipkitės į specialistus.	50 klausimas
		Dažnai	**2**	Patariame Jums skubiai šalinti neigiamus reiškinius juntamus dirbant su kompiuteriu, jei to negalite atlikti patys – kreipkitės į specialistus.	50 klausimas
		Kartais	**1**	Patariame Jums šalinti neigiamus reiškinius juntamus dirbant su kompiuteriu, jei to negalite atlikti patys – kreipkitės į specialistus.	50 klausimas
		Retai	**-**		50 klausimas
50	Ar rūpindamiesi savo kompiuterio saugumu naudojate papildomas priemones (pvz. naudojate programą Ad-Aware Se Personal, Hitman Pro, Spybot - Search & Destroy ir pan.)?	Taip	**-**		Pabaiga, kompiuterinės sistemos saugumo lygis įvertintas.
		Ne	**0,5**		Pabaiga, kompiuterinės sistemos saugumo lygis įvertintas.
51	Ar keičiate savo naudojamą slaptažodį?	Taip	**-**		52 klausimas
		Ne	**2**	Rekomenduojame savo naudojamą slaptažodį keisti, nenaudoti visuomet tokio pačio.	8 klausimas
52	Kaip dažnai keičiate naudojamą slaptažodį?	Dažniau	**-**		8 klausimas
		Kartą į mėn.	**-**		8 klausimas
		Kartą į kelis mėnesius	**-**		8 klausimas
		Kas pusmetį	**0,5**		8 klausimas
		Rečiau	**1**		8 klausimas
53	Ar svarbius duomenis saugote kitame diske nei programas?	Taip	**-**		15 klausimas
		Ne	**5**		15 klausimas

11 lentelės tęsinys

Klausimo Nr.	Klausimas	Galimi atsakymai	Įvertinimas	Patarimas, komentaras	Sekantis klausimas
		Dalį svarbių dokumentų laikau kitame diske nei programos	**2**		15 klausimas
54	Ar Jūsų antivirusinė programinė įranga nustatyta taip, kad maksimaliai apsaugotų kompiuterį (el. pašto skanavimas, kietojo disko reguliarus skanavimas, skanavimas visą laiką)?	Taip	**-**		43 klausimas
		Ne	**2**	Peržiūrėkite savo antivirusinės programos parametrus. Nustatykite juos taip, kad jie maksimaliai apsaugotų duomenis esančius Jūsų kompiuteryje.	43 klausimas
		Ne visada	**0,5**	Peržiūrėkite savo antivirusinės programos parametrus. Nustatykite juos taip, kad jie maksimaliai apsaugotų duomenis esančius Jūsų kompiuteryje.	43 klausimas

Šaltinis: sudaryta darbo autorės.

Apibendrinimas. Sukurta programa buvo duota testuoti žmonėms, kurie vertino savo turimo kompiuterio duomenų daugumo lygį. Buvo apklausti 103 respondentai. Norint, kad programa būtų išsamiai įvertinta programą vertino skirtingo amžiaus žmonės bei skirtingų socialinių grupių žmonės. Atsižvelgiant į vartotojų pastabas buvo pakeistas kelių klausimų formulavimas, įtraukti papildomi klausimai padedantys įvertinti duomenų saugumo lygį kompiuteryje. Siekiant draugiškesnės vartotojo sąsajos programoje padaryti šie pakeitimai: pateikiant rekomendacijas įvesta numeracija, padaryta galimybė ne tik peržiūrėti, bet ir atsispausdinti jas, vartotojas prieš pradėdamas atsakinėti į klausimus yra informuojamas kaip bus pateikiami klausimai bei kaip reikės žymėti tinkamus atsakymus.

3.4. Gauti rezultatai

Gauti rezultatai buvo sugrupuoti į penkis lygmenis (žiūr. 12 lent.), kur pirmas lygmuo yra aukščiausiais balais vertinama duomenų saugumo sistema, o penktasis lygmuo apibūdina kritinio patikimumo duomenų saugą. Norint duomenų apsaugos priemonių vertinimą pateikti vaizdžiau, suprantamiau vartotojui nuspręsta tam panaudoti spalvines išraiškas. Žalia spalva siejama su ramybe, tad tik šia spalva pateikiami atsakymai tik surinkus aukštą saugumo lygio balą. Priešingai, raudona spalva asocijuojasi su pavojais, tad kai duomenų saugumo lygis yra nepakankamo lygio, atsakymai pateikiami šia spalva. Geltona spalva naudojama pateikti vidutinio lygio duomenų saugumo rezultatus, nes ši spalva asocijuojasi su budrumu, atsargumu, tad tarsi savo vartotojui, kad jei nebus imtasi reikiamų veiksmų ateityje galima susidurti su rimtomis duomenų saugumo problemomis.

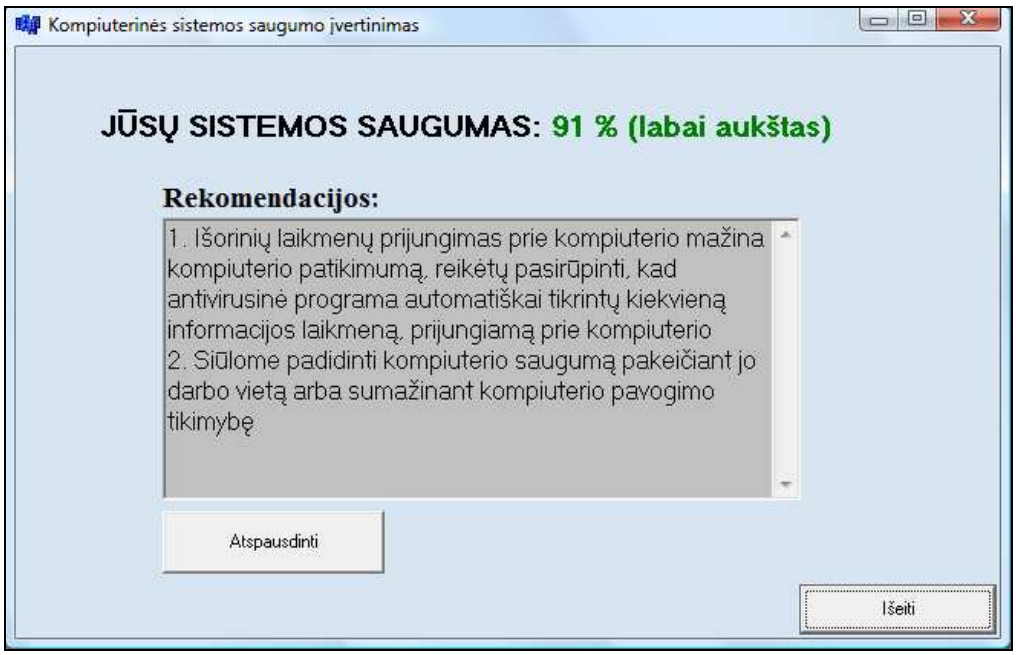
12 lentelė

Duomenų apsaugos priemonių įvertinimas

Patikimumo lygmenys	Įvertinimas	Procentinis įvertinimas (iš 100% galimų)
Pirmas	Kompiuterio saugumo patikimumas yra labai aukšto lygio	80,5-100%
Antras	Kompiuterio saugumo patikimumas yra aukšto lygio	60,5-80%
Trečias	Kompiuterio saugumo patikimumas yra patenkinamo lygio	40,5-60%
Ketvirtas	Kompiuterio saugumo patikimumas yra žemo lygio	20,5-40%
Penktas	Kompiuterio saugumo patikimumas yra kritinio lygio	0-20%

Šaltinis: sudaryta darbo autorės.

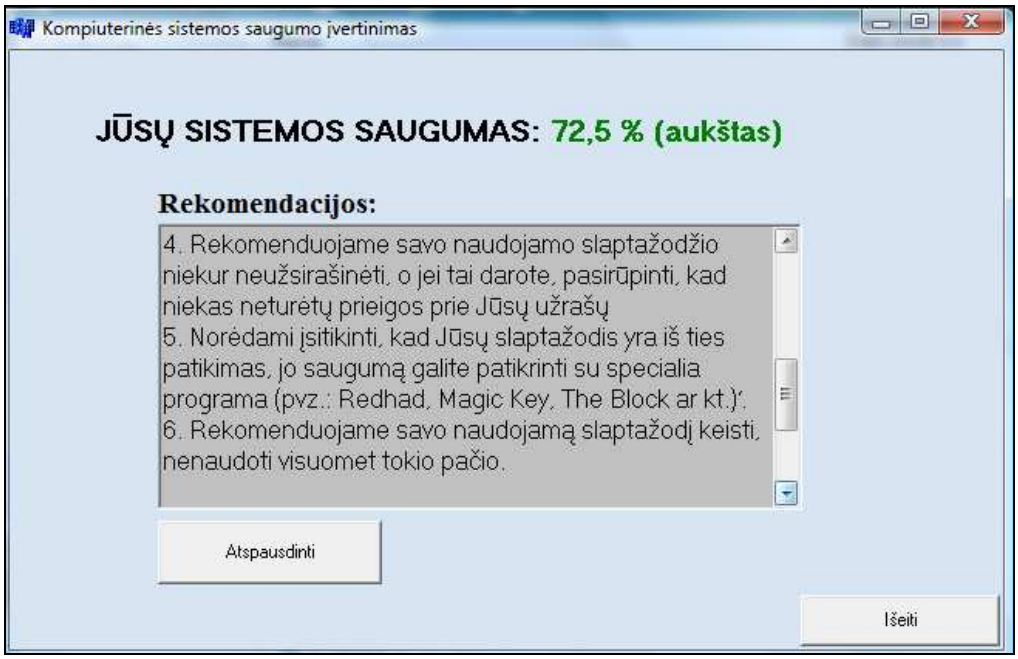
12 lentelėje pateikta klasifikacija yra realizuota praktikoje (žiūr. 7 - 11 pav.). Kai duomenų saugumo lygis yra labai aukštas, įvertinimas pateikiamas žalia spalva bei patarimų kaip pagerinti duomenų saugumą yra sąlyginai mažai (žiūr. 7 pav.).



Šaltinis: sudaryta darbo autorės.

7 pav. Kompiuterio saugumo patikimumas yra labai aukšto lygio

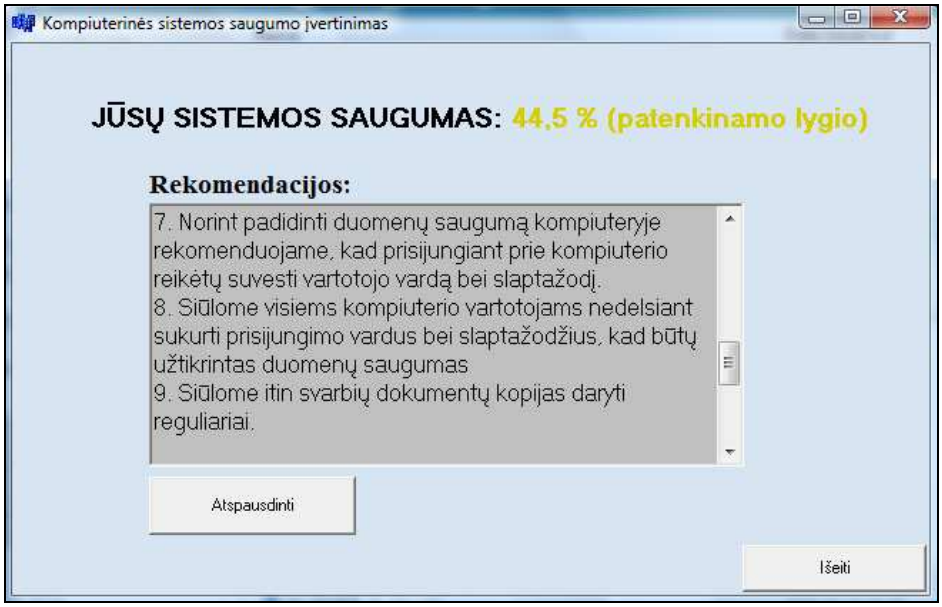
Kai duomenų saugumo lygis yra aukštas, įvertinimas pateikiamas žalia spalva bei patarimų kaip pagerinti duomenų saugumą yra nedaug lyginant su gaunamais patarimais ar rekomendacijomis, kai duomenų saugumo lygis yra kritinio lygio (žiūr. 8 pav.).



Šaltinis: sudaryta darbo autorės.

8 pav. Kompiuterio saugumo patikimumas yra aukšto lygio

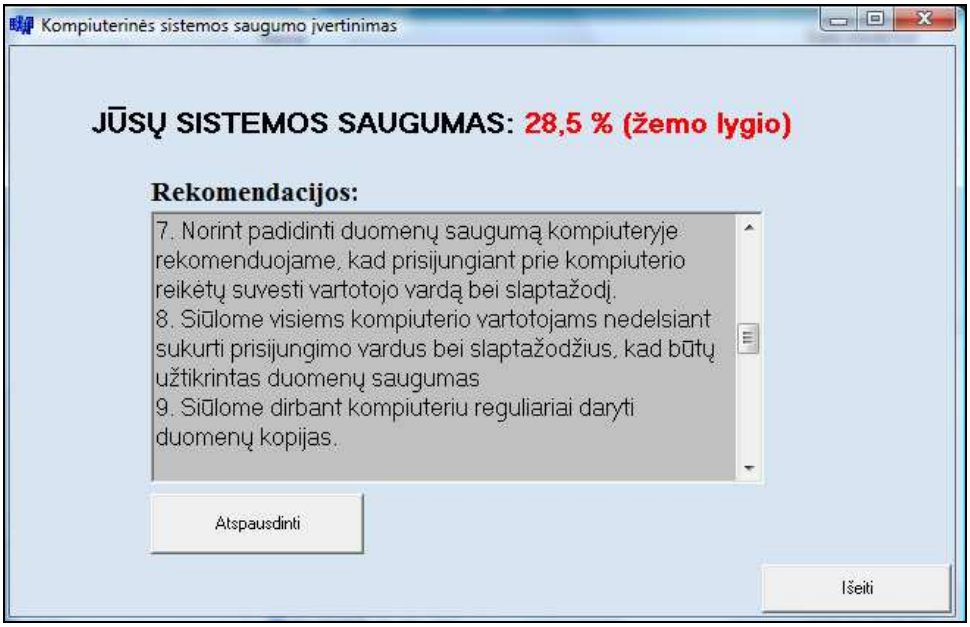
Kai duomenų saugumo lygis yra patenkinamo lygio, įvertinimas pateikiamas geltona spalva bei patarimų kaip pagerinti duomenų saugumą yra pakankamai daug (žiūr. 9 pav.).



Šaltinis: sudaryta darbo autorės.

9 pav. Kompiuterio saugumo patikimumas yra patenkinamo lygio

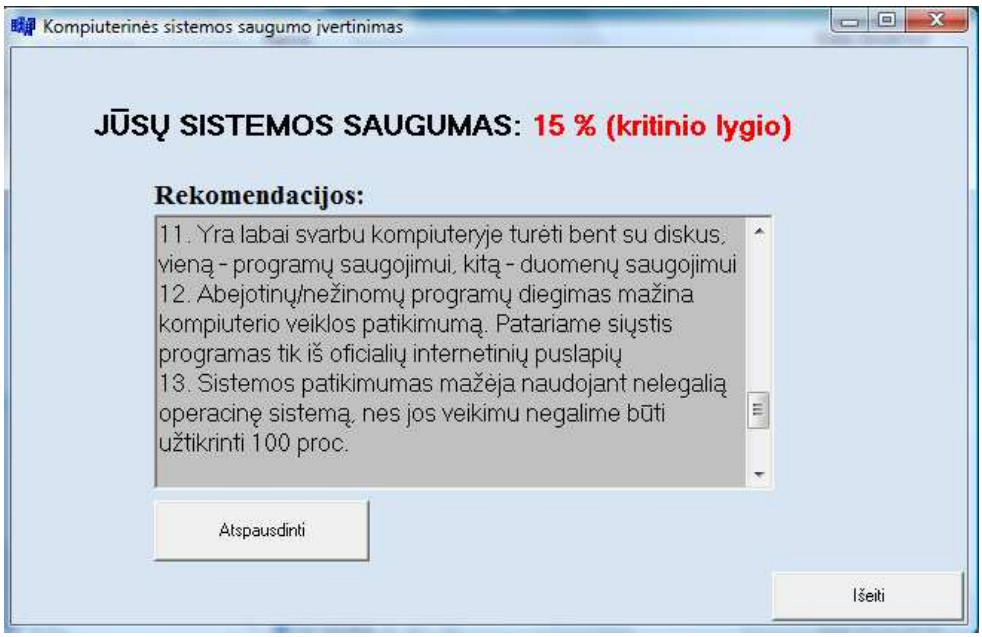
Kai duomenų saugumo lygis yra žemo lygio, įvertinimas pateikiamas raudona spalva bei patarimų kaip pagerinti duomenų saugumą yra daug (žiūr. 10 pav.).



Šaltinis: sudaryta darbo autorės.

10 pav. Kompiuterio saugumo patikimumas yra žemo lygio

Kai duomenų saugumo lygis yra kritinio lygio, įvertinimas pateikiamas raudona spalva bei patarimų kaip pagerinti duomenų saugumą yra labai daug (žiūr. 11 pav.).



Šaltinis: sudaryta darbo autorės.

11 pav. Kompiuterio saugumo patikimumas yra kritinio lygio

3.5. Sukurtos sistemos rezultatų įvertinimas

Sukurtos sistemos palyginimas su duomenų saugumo lygį nustatančiais metodais pateiktas 13 lentelėje. Sukurtą sistemą nuspręsta lyginti būtent su šiais metodais, nes skaičiavimo metodikoje buvo panaudoti šiose metodikose naudojami skaičiavimo būdai (plačiau apie sukurtos sistemos skaičiavimo metodiką 2.1. darbo skyriuje).

13 lentelė

Sukurtos sistemos palyginimas su kitais duomenų saugumą įvertinančiais metodais

Kriterijai/ Metodai	Sukurta saugumo lygį įvertinanti sistema	ISO 15504 standartas	Išlaidų ir gaunamos naudos metodas
Programos kaina	Nemokamai prieinama internete	Kaina svyruoja nuo organizacijos struktūros, oficialiai neskelbiama (vien kursai apie šį standartą kainuoja 2500 Eurų).	Nepateikiama, praktikoje dar nėra įgyvendinta.
Paskirtis	Įvertinti kompiuteryje laikomų duomenų saugumo lygį bei pateikti rekomendacijas, kaip padidinti duomenų saugumo lygį	Kompiuterinių tinklų įvertinimas (galima, bet nepritaikyta tirti pavienio kompiuterio saugumo lygį)	Kompiuterinių tinklų įvertinimas (galima, bet nepritaikyta tirti pavienio kompiuterio saugumo lygį)
Prieinamumas	Pavienių kompiuterių vartotojams.	Organizacijoms	Organizacijoms
Įvertinimas ar kompiuteris turi išeigą į internetą	+	+	+
Antivirusinės programos būvimo įvertinimas	+	+	+
Antivirusinės programos saugumo įvertinimas	+	+	+
Kompiuterio naudotojų įvertinimas	+	+	+
Slaptažodžio būvimo įvertinimas	+	+	+
Slaptažodžio saugumo įvertinimas	+	+	+
Duomenų kopijų darymo įvertinimas	+	+	+
Duomenų kopijų laikymo vietos saugumo įvertinimas	+	-	-
Operacinės sistemos įvertinimas	-	+	+
Itin svarbių dokumentų turėjimo įvertinimas	+	?	-
Įvertinimas ar dokumentai yra laikomi kitame diske nei programos	+	+	+

13 lentelės tęsinys

Kriterijai/ Metodai	Sukurta saugumą vertinanti programa	ISO 15504 standartas	Išlaidų ir gaunamos naudos metodas
Subjektyvių dalykų įvertinimas	+	-	-
Operacinės sistemos legalumo įvertinimas	+	+	+
Naudojamų programų legalumo įvertinimas	+	+	+
Įvertinimas ar yra atidarinėjami nežinomų siuntėjų siunčiami laiškai	+	+	-
Kompiuterio laikymo vietos įvertinimas	+	?	+
Virusų įtakos kompiuteriui įvertinimas	+	+	-
Išorinių informacijos laikmenų naudojimo įvertinimas	+	+	+
Kompiuterio būklės įvertinimas	+	+	+
Papildomų sąlygų įvertinimas dirbant su kompiuteriu	+	+	+
Pateikiami patarimai kaip padidinti duomenų saugumo lygį	+	-	-
Procentinis įvertinimas (100% skalėje)	19	15-17	15

Šaltinis: sudaryta darbo autorės.

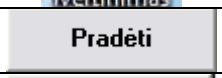
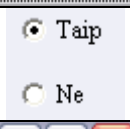
Apibendrinimas. Sukurta sistema pagal duomenų saugumo nustatymo procesus buvo palyginta su analogais. Sukurtos sistemos pranašumas - tai padarytų duomenų kopijų laikymo vietos įvertinimas, kompiuterio įvertinimas, itin svarbių dokumentų turėjimo įvertinimas, subjektyvių dalykų dirbant su kompiuteriu įvertinimas.

3.6. Programos vadovas

Sistema gali naudotis ir nedidelį kompiuterinį raštingumą turintys kompiuterio vartotojai, nes programos funkcijos yra apgalvotos ir išdėstytos kuo suprantamiau bei paprasčiau. Duomenų įvedinėti klientui į sistemą nereikia, tereikia iš galimų atsakymo variantų pasirinkti labiausiai tinkamą. Atsakinėjant į klausimus nėra ribojamas laikas, kiek galima jo sugaišti atsakant į konkretų klausimą, tiesiog atsakius į klausimą ir paspaudus mygtumą toliau – vartotojui bus pateikiamas sekantis klausimas ir galimybės grįžti atgal bei pataisyti atsakymą į prieš tai pateiktą klausimą nebebus. Norint paleisti programą, reikia paleisti failą: „Duomenu saugumo ivertinimas“. Supratus, kad į klausimą buvo atsakyta neteisingai vienintelė galimybė nutraukti atsakinėjimą į klausimus bei pradėti atsakinėjimą iš naujo. Tad prieš spaudžiant mygtuką „Toliau>“ reikia pasitikrinti ar pasirinktas tikrai tinkamas atsakymas. Daugiau apie sistemos naudojamus mygtukus 14 lentelėje.

14 lentelė

Sistemos naudojamų mygtukų paaiškinimas

Naudojami mygtukai	Paaiškinimas
	Programos paleidimo failas.
	Mygtukas naudojamas pirmame programos lange pradedant darbą su programa.
	Kiekviename programos lange yra galimybė nutraukti duomenų saugos lygio įvertinimą, tereikia paspausti mygtuką „Išeiti“.
	Mygtukas naudojamas paskutiniajame programos lange kai vartotojui suteikiama galimybė ne tik peržiūrėti, bet ir atsispausdinti rekomendacijas bei patarimus.
	Atsakius į sistemos pateiktą klausimą ir norint pereiti prie sekančio klausimo – reikia paspausti mygtuką „Toliau>“.
	Atsakant į klausimus vartotojas turi galimybę pasirinkti tik vieną iš pasirinktų variantų.
	Sistema taip pat naudoja tradicinius Windows aplinkos mygtukus: minimizuoti, maksimizuoti, uždaryti.

Šaltinis: sudaryta darbo autorės.

Sistemoje naudojami mygtukai yra lengvai suprantami, nes ant jų yra parašytas veiksmas, kurį jie daro, kai juos paspaudžiame. Klausimai bei pranešimai vartotojui (žiūr. 1 priedą) yra pateikiami lietuvių kalba, tad vartotojas gali lengvai suprasti, ko jo klausia programa.

Kiek klausimų pateiks sistema vartotojui prieš pradedant vartotojui atsakinėti į klausimus negalima atsakyti, nes sistemos sekantis klausimas priklauso nuo ką tik vartotojo pasirinktų

atsakymo varianto. Tad prieš pradedant atsakinėti į sistemos klausimus visuomet verta pagalvoti ar turite pakankamai laisvo laiko, kad į klausimus galėtumėte atsakyti apgalvotai bei neskubant.

Iš viso yra galimi penki sistemos pateikiami duomenų saugos lygio įvertinimai (žiūr. 7 - 11 paveikslėlius) nuo kritinio saugumo lygio iki labai aukšto. Sistema saugumo lygį vertina 100 balų sistemoje.

Apibendrinimas. Sistema gali naudotis ir nedidelį kompiuterinį raštingumą turintys kompiuterio vartotojai, nes programos funkcijos yra apgalvotos ir išdėstytos kuo suprantamiau bei paprasčiau, taip pat programos vadove yra aprašyti naudojami mygtumai.

3.7. Ekspertinės sistemos realizavimo išvados

Vertinant duomenų apsaugos priemones, pasirinkta kompiuterinę sistemą vertinti šiais aspektais: slaptažodžio buvimas (jo saugumas), antivirusinės programos buvimas (jos saugumas), operacinės sistemos, naudojamų programų legalumas, „šiukšlių" patekimo į kompiuterį rizikos įvertinimas, ugniasienės buvimas (jei kompiuteris turi išeigą į internetą), vartotojų (-o) besinaudojančių (-io) kompiuteriu patikimumas ir t.t. Vertinant kompiuterinę sistemą yra atsižvelgiama ne tik į kompiuteryje įdiegtas programas, jų legalumą, bet ir į vartotojo atliekamus veiksmus.

Grėsmės, keliančios pavojų duomenų esančių kompiuteryje saugumui buvo identifikuotos ir sugrupuotos. Remiantis grėsmių svoriais buvo sukurta ekspertinė sistema, kuri net tik vertina duomenų saugumo priemonių saugumo lygį, bet ir pateikia patarimus klientui, kaip padidinti duomenų saugumo lygį. Ekspertinei sistemai sukurti naudota programavimo kalba C++.

Atsakius į sistemos pateikiamus klausimus yra gaunamas vienas iš penkių galimų atsakymų, įvertinantis duomenų saugumo priemonių lygį skalėje nuo 0 iki 100 proc. sistemoje (vartotojui taip pat pateikiamas žodinis įvertinimas nuo kritinio vertinimo iki labai aukšto sistemos saugumo vertinimo). Rezultatai yra pateikiami ne tik skaitine, bet ir žodine išraiška bei pateikiami pasiūlymai, kokių konkrečių veiksmų reikia imtis, kad duomenų esančių kompiuteryje saugumo lygis būtų didesnis. Norint duomenų apsaugos priemonių vertinimą pateikti vaizdžiau, suprantamiau vartotojui nuspręsta tam panaudoti spalvines išraiškas.

Sukurta programa buvo ištestuota. Buvo apklausti 103 respondentai. Norint, kad programa būtų išsamiai įvertinta programą vertino skirtingo amžiaus žmonės bei skirtingų socialinių grupių žmonės. Atsižvelgiant į vartotojų pastabas buvo pakeistas kelių klausimų formulavimas, įtraukti papildomi klausimai padedantys įvertinti duomenų saugumo lygį kompiuteryje. Siekiant draugiškesnės vartotojo sąsajos programoje padaryti šie pakeitimai: pateikiant rekomendacijas įvesta numeracija, padaryta galimybė ne tik peržiūrėti, bet ir atsispausdinti jas, vartotojas prieš

pradėdamas atsakinėti į klausimus yra informuojamas kaip bus pateikiami klausimai bei kaip reikės žymėti tinkamus atsakymus.

Sukurta sistema pagal duomenų saugumo nustatymo procesus buvo palyginta su analogais. Sukurtos sistemos pranašumas - tai galimybė net neišeinant iš namų ir be papildomų lėšų įvertinti duomenų saugumo lygį, esantį kompiuteryje bei išsiaiškinti kokių konkrečių žingsnių reikia imtis didinant patikimumo lygį. Norint įvertinti duomenų saugumo lygį su šia sistema nereikia turėti daug žinių apie saugumo nustatymo metodikas (tereikia atsakyti į paprastus sistemos pateikiamus klausimus). Sukurta sistema palengvina kompiuterio vartotojų dedamas pastangas išsiaiškinti duomenų saugumo lygį esantį kompiuteryje bei taupo laiką, skiriamą saugumo lygio pagerinimui.

Atsižvelgiant į programos vartotojų poreikius ateityje programos veikimo spektras gali būti plečiamas ir pritaikytas ne tik pavienio kompiuterio vertinimui, bet ir kompiuterinės sistemos saugumo vertinimui.

IŠVADOS IR PASIŪLYMAI

1. Didėjant kompiuterinių duomenų apimtims ir augant vartotojų priklausomybei nuo jų, duomenų saugumo klausimas tampa vis aktualesnis. Vartotojui vis aktualiau žinoti, ne tik kaip apsaugoti savo duomenis, bet ir kaip padaryti jų lygį patikimesniu.

2. Vartotojui yra labai svarbu kiekybiškai įvertinti savo kompiuterinės sistemos saugumo lygį. Pastaruoju metu naudojami metodai bei priemonės dažniausiai įvertina arba atskiras galimo naudoti duomenų saugumo rinkinio dalis, arba jos skirtos duomenų saugos specialistams, bet ne kompiuterinės sistemos vartotojams.

3. Šiuo metu naudojamos duomenų saugumo lygio vertinimo metodikos turi eilę trūkumų: a) dažniausiai nėra atliekamas kiekybiniai vertinimai, juose neišvengiama subjektyvumų; b) pateikiamų įvertinimų rezultatų analizė yra sudėtinga; c) pateikiami rezultatai dažniausiai nenurodo konkrečių veiksmų, kurie reikalingi padidinti naudojamos sistemos saugumo lygį.

4. Apibrėžtos kompiuterinių duomenų apsaugos būdų ir priemonių rinkinio atitinkamos grupės bei jų įtaka saugumo lygiui.

5. Pasiūlyta ekspertinės sistemos, leidžiančios kiekybiškai įvertinti duomenų saugumo lygį bei parenkančios rekomendacijas jo didinimui, struktūra.

6. Realizuotas bei išsamiai ištestuotas ekspertinės sistemos prototipas, kuris yra orientuotas į kompiuterio vartotoją. Sukurta sistema palengvina kompiuterio vartotojo dedamas pastangas išsiaiškinti duomenų saugumo lygį esantį kompiuteryje bei taupo laiką, skiriamą saugumo lygio pagerinimui.

7. Siekiant pagrindinio tikslo, sukurti ekspertinę sistemą, kuri įvertintų kompiuterinių duomenų apsaugos priemonių rinkinio saugumo lygį ir teiktų rekomendacijas saugumo lygio padidinimui, darbe yra įvykdyti išsikelti uždaviniai: išnagrinėti rizikos faktoriai bei apsaugos būdai nuo jų, išanalizuoti duomenų apsaugos sistemos įvertinimo metodai, pasiūlyta ir sukurta ekspertinė sistema, įvertinanti duomenų apsaugos priemonių rinkinio patikimumo lygį, realizuotas sistemos prototipas, orientuotas į atskiro kompiuterio naudojamų saugos priemonių įvertinimą, ištestuoti bei įvertinti sukurtos sistemos rezultatai.

8. Darbe duomenys pateikti apdoroti ir susisteminti, kur įmanoma informacija pateikta lentelėse ar schemose, kad būtų lengva susidaryti vaizdą apie kuriamą sistemą bei analizuojamus metodus.

9. Sukurta sistema galėtų būti tobulinama šiais pagrindiniais aspektais: a) pritaikyta vertinti ne tik atskiriems kompiuteriams, bet ir jų tinklams; b) vertinant būtų atsižvelgiama į papildomus parametrus: finansinius, laikinius ir pan.

LITERATŪRA

MOKSLINĖ LITERATŪRA

1. BUTLER, Shawn A. (2002) Security Attribute Evaluation Method: A Cost-Benefit Approach [interaktyvus]. [žiūrėta 2008 m. vasario 26 d.]. Prieiga per internetą <http://portal.acm.org/citation.cfm?id=581370 >;
2. DUNCAN, George T.; KELLER-MCNULTY, Salvie A.; ir STOKES, S. Lynne. (2004) Data Utility through the R-U Confidentiality Map [interaktyvus]. [žiūrėta 2008 m. balandžio 15 d.]. Prieiga per internetą <http://www.niss.org/technicalreports/tr121.pdf>;
3. GORDON, Sarah. (2004) A Short Course in Antivirus Software Testing: Seven Simple Rules for Evaluating Tests. Prieiga internete [interaktyvus]. [žiūrėta 2008 m. kovo 21 d.]. Prieiga per internetą: <http://securityresponse.symantec.com/avcenter/reference/AntivirusSoftwa re_Testing.pdf>;
4. JAMUKOWICZ, Sławomir, KOWAL, Tomasz, KWIECIEN, Agnieszka (2003) Bezpieczeństwo w sieci Unexpected [interaktyvus]. [žiūrėta 2007 m. rugsėjo 12 d.]. Prieiga per internetą <http://www.wcss.wroc.pl/wcss/infor/ak/bezp.html>;
5. MEHROTRA, S.; BUTTS, C, KALASHNIKOV, D.; VENKATASUBRAMANIAN, N. (2004) Project Rescue: Challenges in Responding to the Unexpected [interaktyvus]. [žiūrėta 2007 m. rugsėjo 02 d.]. Prieiga per internetą <http://www.ics.uci.edu/~dvk/pub/SPIE04_dvk.pdf >;
6. SAYCIER, G. BELLON, C. (2006) VLSI Test Expertise System Using a Control Flow [interaktyvus]. [žiūrėta 2009 m. vasario 14 d.]. <Modelhttp://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1585844>;
7. TREACY, Bridget C. (2007) Merkblatt Lawinendienst:Beurteilung lokale Lawinengefährdung und Dokumentation [interaktyvus]. [žiūrėta 2008 m. balandžio 20 d.]. Prieiga per internetą <http://www.sils-ch.ch/doc/MerkblattDokumentation.pdf>;
8. Von HIPPEL, Eike. (2007) Verbraucherschutz [interaktyvus]. [žiūrėta 2008 m. kovo 26 d.]. Prieiga per internetą <http://books.google.lt/books?id=XLGys674zuIC&pg=PA76&lpg=PA76&dq=Gefahrenstufe+Daten&source=bl&ots=mFzJ9KW_A_x&sig=62GibYOEptTLEtA8uIMXRWpPZWc&hl=lt&ei=484USuW4FI_Gsga-z-icCg&sa=X&oi=book_result&ct=result& resnum=2#PPP1,M1>;

9. Шнайер, Б. (2003) Секреты и ложь. Безопасность данных в цифровом мире [interaktyvus]. [žiūrėta 2008 m. balandžio 29 d.]. Prieiga per internetą <http://www.ozon.ru/context/detail/id/1485455/>;

INFORMACIJOS ŠALTINIAI

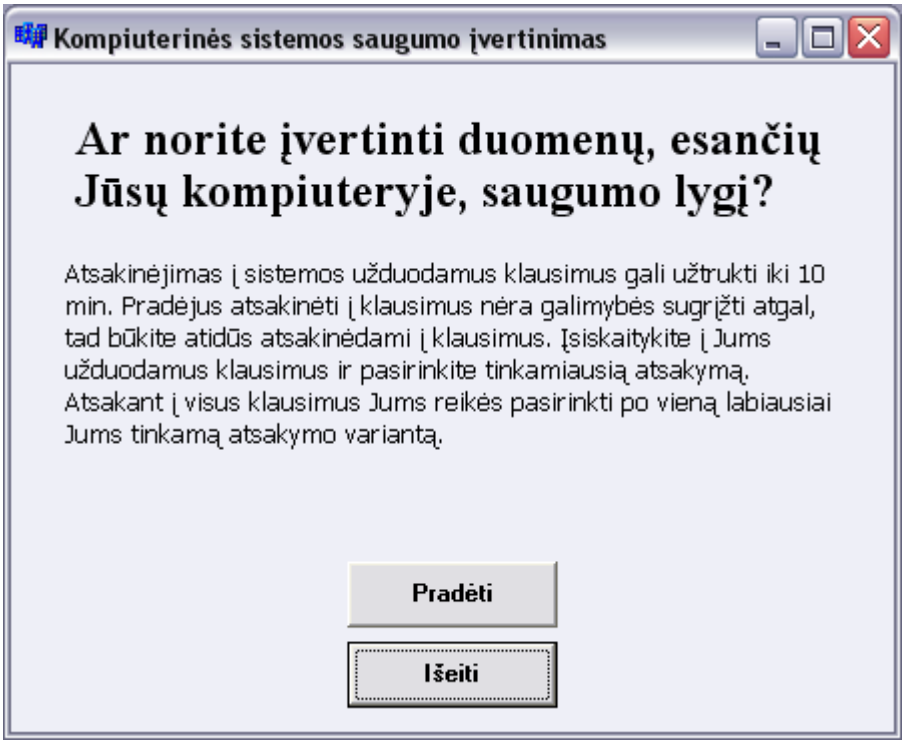
10. Amazon.com. (2008) [interaktyvus]. [žiūrėta 2008 m. balandžio 21 d.]. Prieiga per internetą <http://www.amazon.com/estimators-automated-automobile-insurance-estimation/dp/B00 092L62K >;
11. БУДИК, Александр. (2009) компьютеропline Хорошо ли защищены ваши данные? [interaktyvus]. [žiūrėta 2008 m. sausio 23 d.]. Prieiga per internetą <http://www.computerra.ru/hitech/231074/>.
12. Blekinge Tekniska Hogskola. (2009) [interaktyvus]. [žiūrėta 2009 m. Gegužės 7 d.]. Prieiga per internetą <http://www.bth.se/fou/cuppsats.nsf/bbb56322b274389dc1256608004f052b/33ea02dad9a9b1bec1256c3600535312!OpenDocument>;
13. Dorling, Alec. (2008) ISO SPICE [interaktyvus]. [žiūrėta 2008 m. lapkričio 29 d.]. Prieiga per internetą < http://www.isospice.com/authors/1/Alec-Dorling >;
14. DRG (Data Recovery Group). (2007) [interaktyvus]. [žiūrėta 2007 m. spalio 23 d.]. Prieiga per internetą <http://www.datarecoverygroup.com>;
15. DriveSavers Data Recovery. (2008) [interaktyvus]. [žiūrėta 2008 m. sausio 20 d.]. Prieiga per internetą <http://www.drivesavers.com>;
16. Earth and Planetary Science Letters. (2008) [interaktyvus]. [žiūrėta 2008 m. gegužės 17 d]. Prieiga per internetą http://www.sciencedirect.com/science?_ob=ArticleUR L&_udi=B6V61-4K66F58-1&_user=10&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=93e1cb5d54ffdced5639878ce4dac19b >;
17. Electronic Orange Book. (2008) [interaktyvus]. [žiūrėta 2008 m. balandžio 17 d]. Prieiga per internetą <http://www.fda.gov/cder/ob/>;
18. eSecurity. (2006) [interaktyvus]. [žiūrėta 2008 m. kovo 11 d.]. Prieiga per internetą <http://www.esecurity.lt/article/2053.html>;
19. Ezine article. (2008) [interaktyvus]. [žiūrėta 2008 m. vasario 20 d.]. Prieiga per internetą <http://ezinearticles.com/?The-Importance-of-Computer-Security&id=146652>;
20. Freepatentsonline. (2009) [interaktyvus]. [žiūrėta 2009 m. Gegužės 7 d.]. Prieiga per internetą <http://www.freepatentsonline.com/6791628.html>;

21. GIMŽAUSKAS, Gintaras. (2009) Computer act!ve. Sutalpink daugiau failų, Nr. 5. Vilnius, p. 20-22;
22. Informacijos saugos sprendimai. (2008) [interaktyvus]. [žiūrėta 2008 m. lapkričio 29 d.]. Prieiga per internetą <www.isec.lt>;
23. ISO 27001 Security. (2008) [interaktyvus]. [žiūrėta 2008 m. sausio 21 d.]. Prieiga per internetą <http://www.27001-online.com/>;
24. YAKARIS, Deksny. (2009) Lietuvos rytas. Piratų valdos išsiplėtė, Nr. 112 (5575). Vilnius, p. 9;
25. JAKAS Dainius. (2008) Naujoji komunikacija. Internetinių grėsmių plėtra per pirmąjį 2008m. pusmetį, Nr. 11 (227). Vilnius, p. 10;
26. KATZ, Jonathon, MERIER, Robert J. (2005) Linux + Windows how to [interaktyvus]. [žiūrėta 2009 m. sausio 11 d.]. Prieiga per internetą <http://tldp.org/HOWTO/Linux+Win dows-HOWTO/ >;
27. Kuhn, Markus. (1999) International standart date and time notation [interaktyvus]. [žiūrėta 2008 m. kovo 20 d.]. Prieiga per internetą <http://www.cl.cam.ac.uk/~mgk25/iso-time.html>;
28. Lehigh University. (2009) [interaktyvus]. [žiūrėta 2009 m. Gegužės 7 d.]. Prieiga per internetą <http://www.lehigh.edu/security/computepolicy.html>;
29. LEŠČINSKAS, Liutauras (2009) Verslo klasė. Sudrausmintos laisvės saldumas, Nr. 6 (85). Vilnius, p. 46-49;
30. Mbone:Multicasting Tomorrow‘s Internet. (2008) [interaktyvus]. [žiūrėta 2009 m. Gegužės 9 d.]. Prieiga per internetą <http://www.savetz.com/mbone/>;
31. PC Tools. (2008) [interaktyvus]. [žiūrėta 2008 m. sausio 10 d]. Prieiga per internetą <http://www.pctools.com/guides/password>;
32. RFid Gazette. (2007) [interaktyvus]. [žiūrėta 2009 m. balandžio 24 d.]. Prieiga per internetą <http://www.rfidgazette.org/2007/04/rfid_implants_5.html>;
33. Rutgers secure. Risk Assessment. (2008) [interaktyvus]. [žiūrėta 2008 m. balandžio 19 d.]. Prieiga per internetą <http://rusecure.rutgers.edu/sec_plan/risk.php>;
34. Scribd. (2009) [interaktyvus]. [žiūrėta 2009 m. balandžio 10 d.]. Prieiga per internetą <http://www.scribd.com/doc/429542/Read-This-Av-Compare>;
35. SecureWorks. (2009) [interaktyvus]. [žiūrėta 2009 m. Gegužės 9 d.]. Prieiga per internetą <http://www.secureworks.com/research/articles/firewall-security/>;
36. SKROBIKAS, Martynas. (2009) Computer Bild Lietuva. Nauja „Linux“ – daug greitesnė, Nr. 9. Vilnius, p. 5;

37. Softweare Quality. (2008) [interaktyvus]. [žiūrėta 2008 m. birželio 15 d.]. Prieiga per internetą <http://software-quality.blogspot.com/2006/10/risk-based-selection-for-gile.html>;
38. ŠILKONAS, Gediminas. (2009) Kompiuterija. Apsaugokite nešiojamame kompiuteryje esančią informaciją nuo vagystės. Nr. 5 (129). Vilnius, p. 32-33;
39. The Engineering ToolBox. (2005) [interaktyvus]. [žiūrėta 2008 m. balandžio 04 d.]. Prieiga per internetą <http://www.engineeringtoolbox.com/clean-rooms-iso-d_933.html>;
40. The World Wide Web Security. (2004) [interaktyvus]. [žiūrėta 2007 m. lapkričio 13 d.]. Prieiga per internetą <http://www.w3.org/Security/faq/www-security-faq.html>;
41. U.S. Bureau of Labor Statistics. (2008) [interaktyvus]. [žiūrėta 2008 m. gegužės 23 d.]. Prieiga per internetą <http://www.bls.gov/oes/current/oes151051.htm>;
42. VeriSign. (2008) [interaktyvus]. [žiūrėta 2008 m. vasario 24 d.]. Prieiga per internetą <http://www.verisign.com/authentication/individual-authentication/digital-id/index.html>;
43. Voting Matters. (2000) [interaktyvus]. [žiūrėta 2008 m. kovo 29 d.]. Prieiga per internetą <http://www.votingmatters.org.uk/ISSUE12/P1.HTM>.

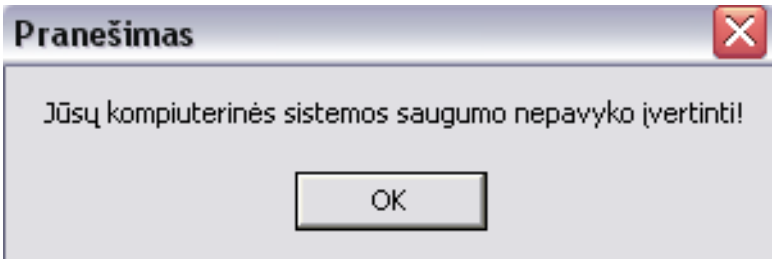
1 PRIEDAS

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

12 pav. Kompiuterinės sistemos saugumo įvertinimo pradinė lentelė



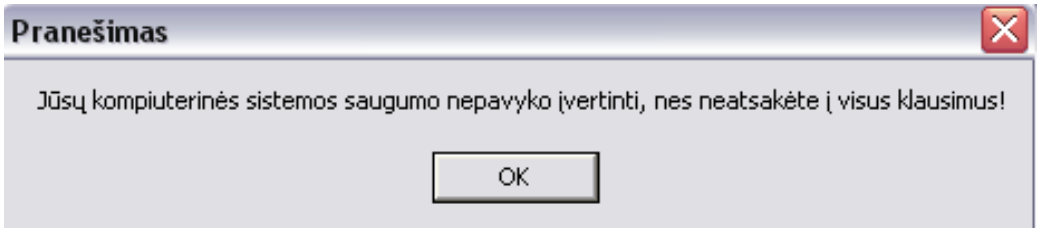
Šaltinis: sudaryta darbo autorės.

13 pav. Pranešimas iškrentantis atsisakius atsakinėti į sistemos pateikiamus klausimus

Duomenų saugos įvertinimo programos lentelės bei pranešimai

Šaltinis: sudaryta darbo autorės.

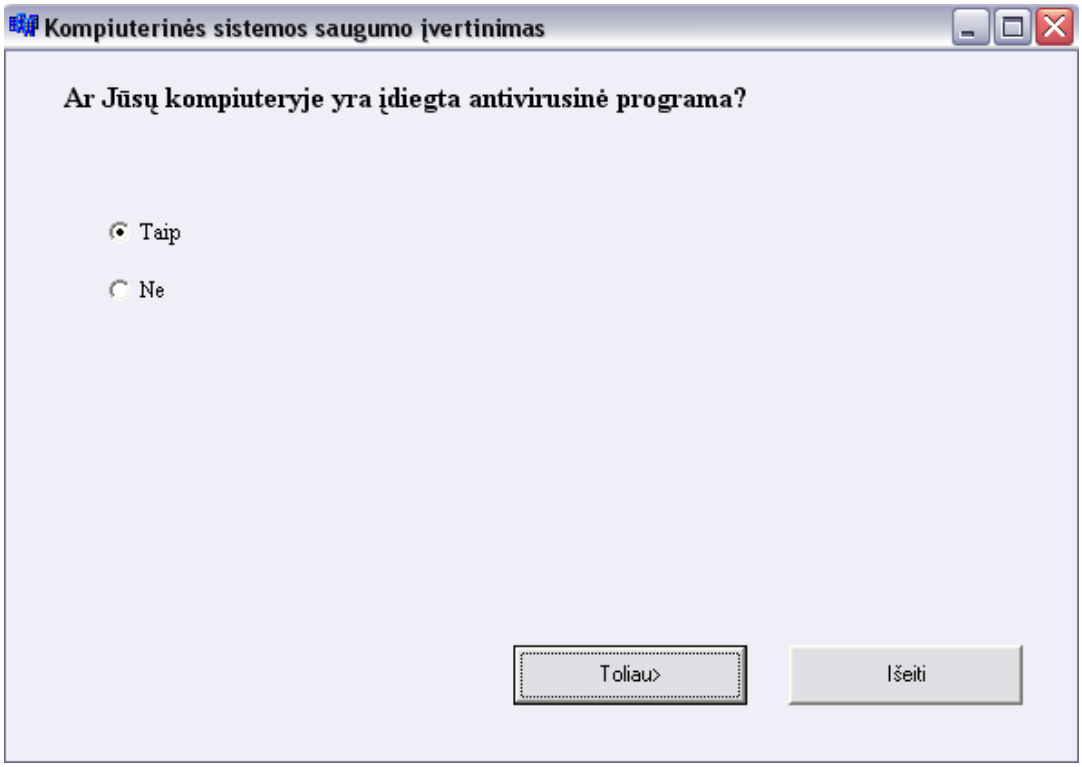
14 pav. Interneto ryšio turėjimo įvertinimas



Šaltinis: sudaryta darbo autorės.

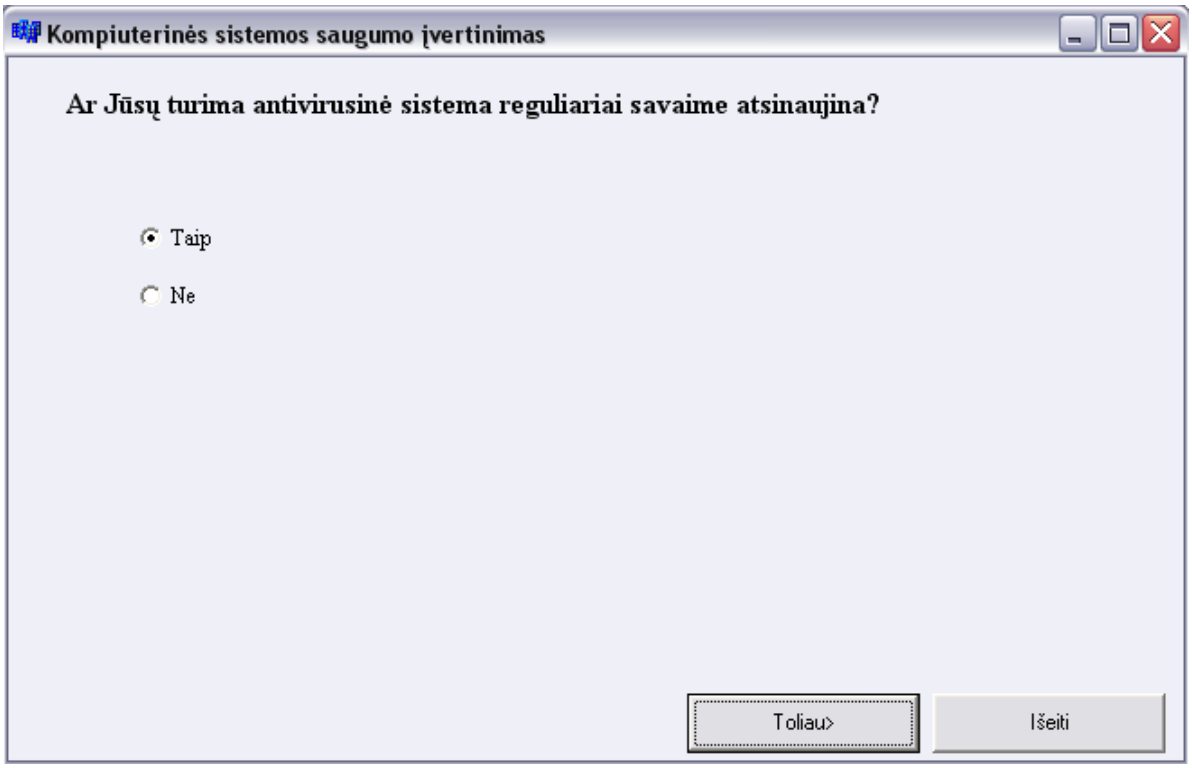
15 pav. Pranešimas iškrentantis neatsakius į visus sistemos pateikiamus klausimus

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

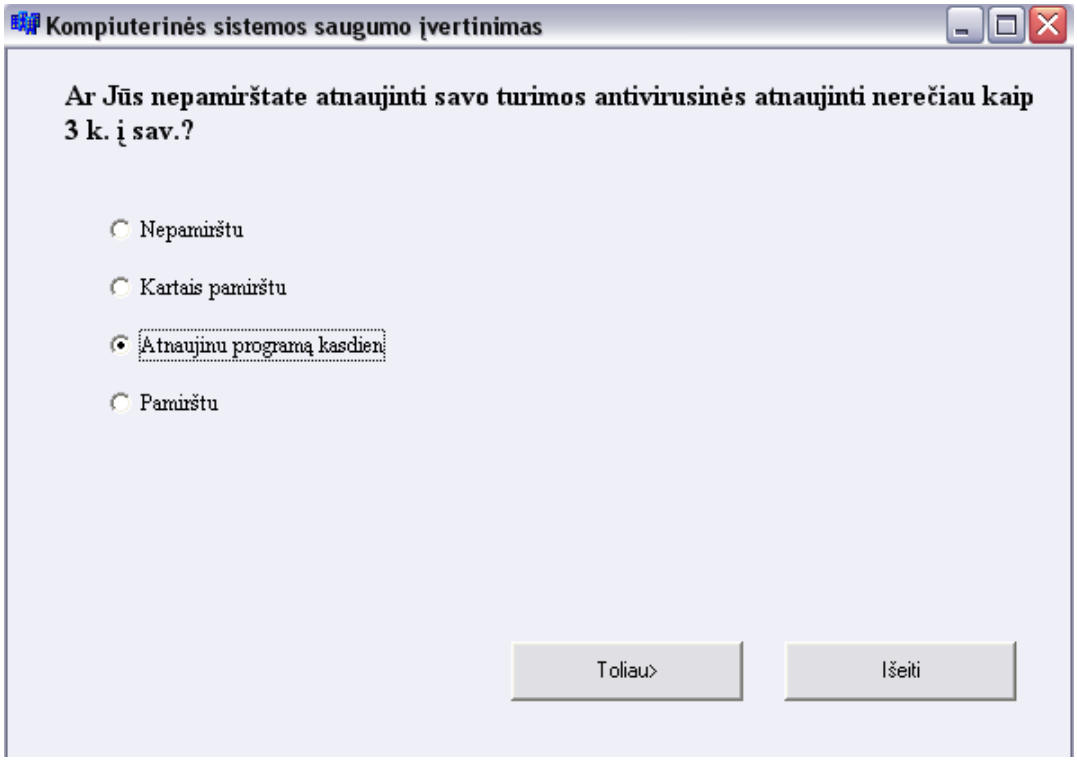
16 pav. Antivirusinės sistemos būvimo įvertinimas



Šaltinis: sudaryta darbo autorės.

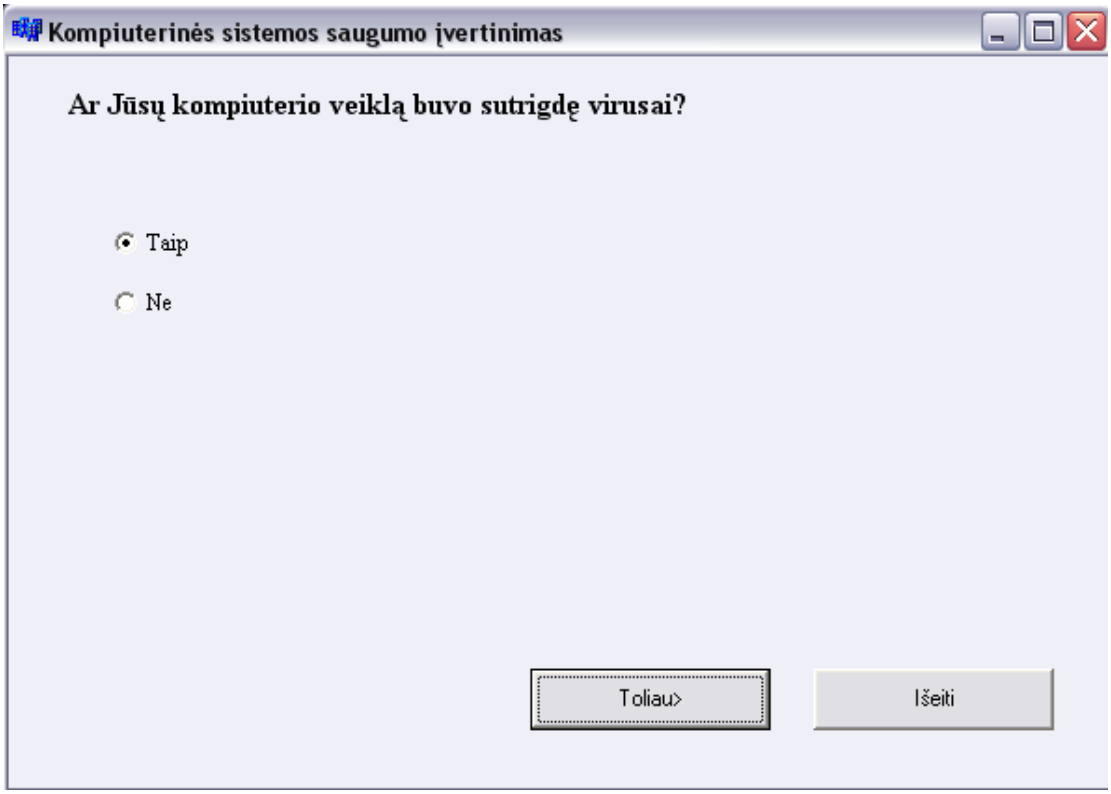
17 pav. Antivirusinės sistemos veikimo įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

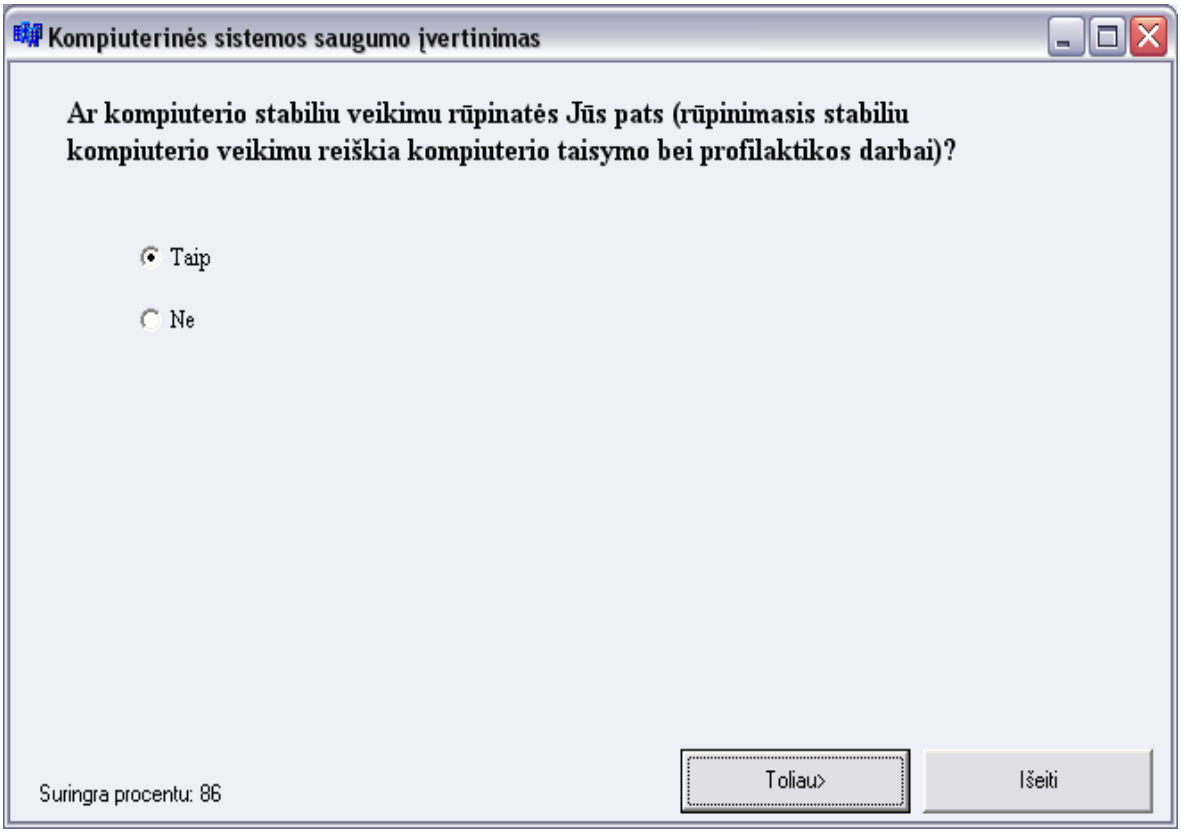
18 pav. Vartotojo atliekamų veiksmų su antivirusine sistema įvertinimas



Šaltinis: sudaryta darbo autorės.

19 pav. Virusų grėsmės įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



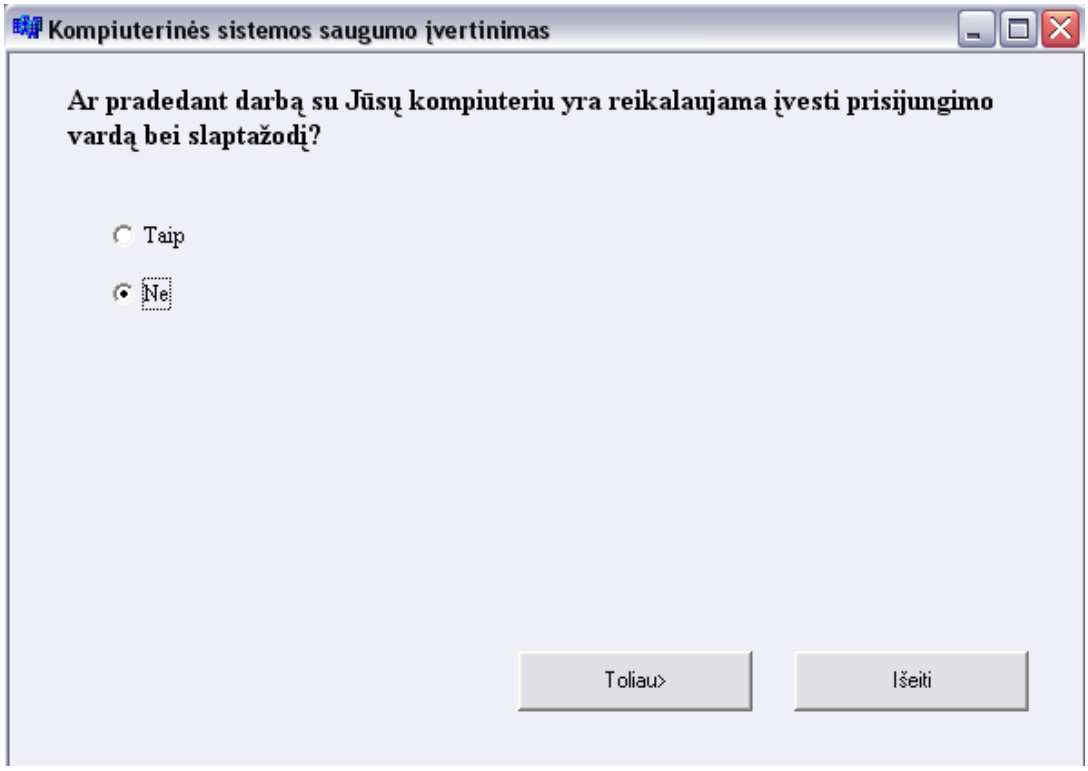
Šaltinis: sudaryta darbo autorės.

20 pav. Kompiuterio saugomo užtikrinimas

Šaltinis: sudaryta darbo autorės.

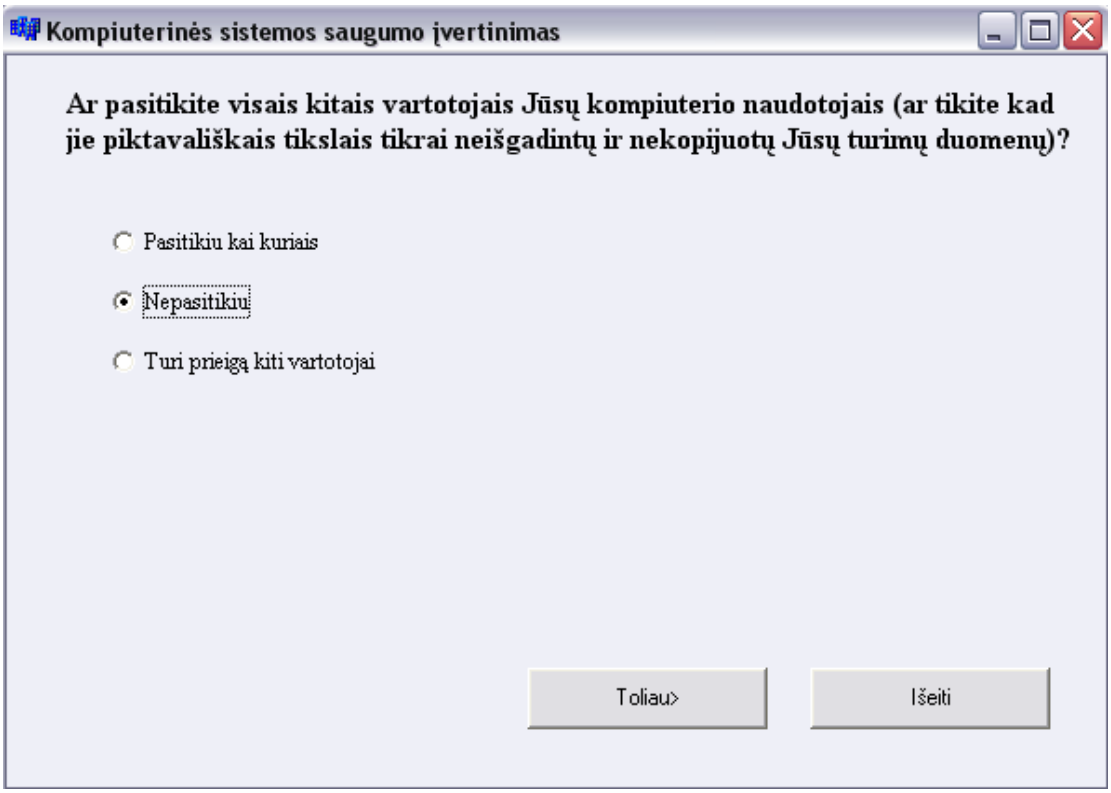
21 pav. Vartotojo kompetencijos įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

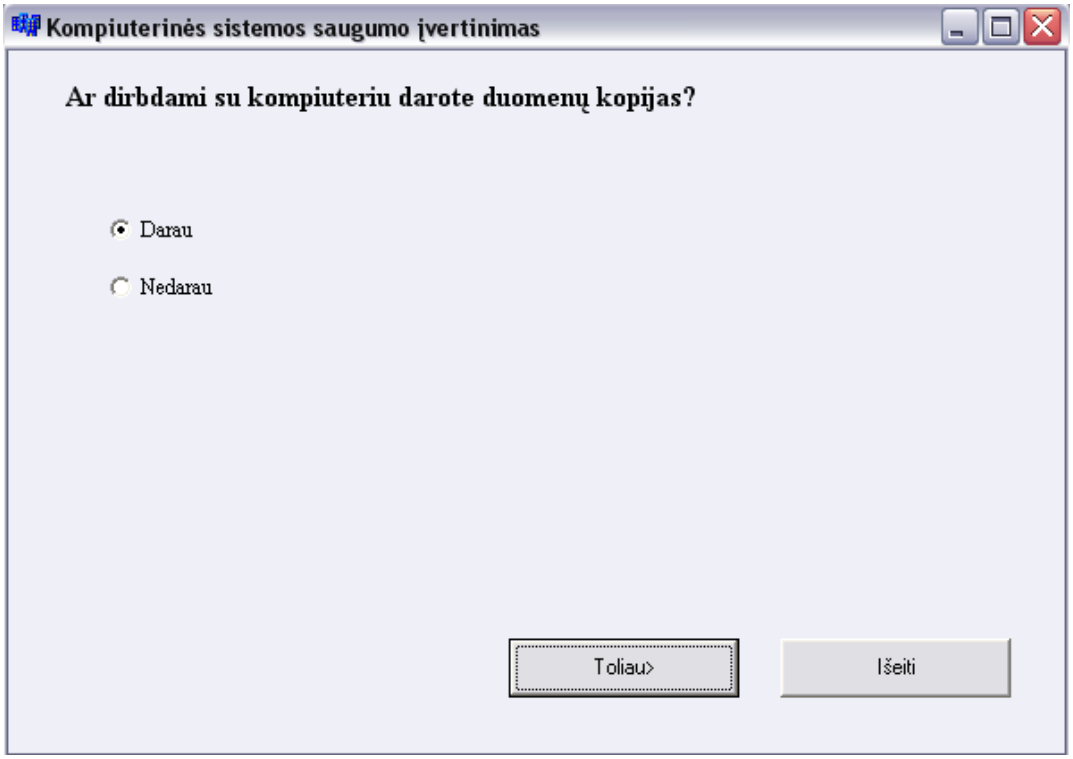
22 pav. Slaptažodžio būvimo įvertinimas



Šaltinis: sudaryta darbo autorės.

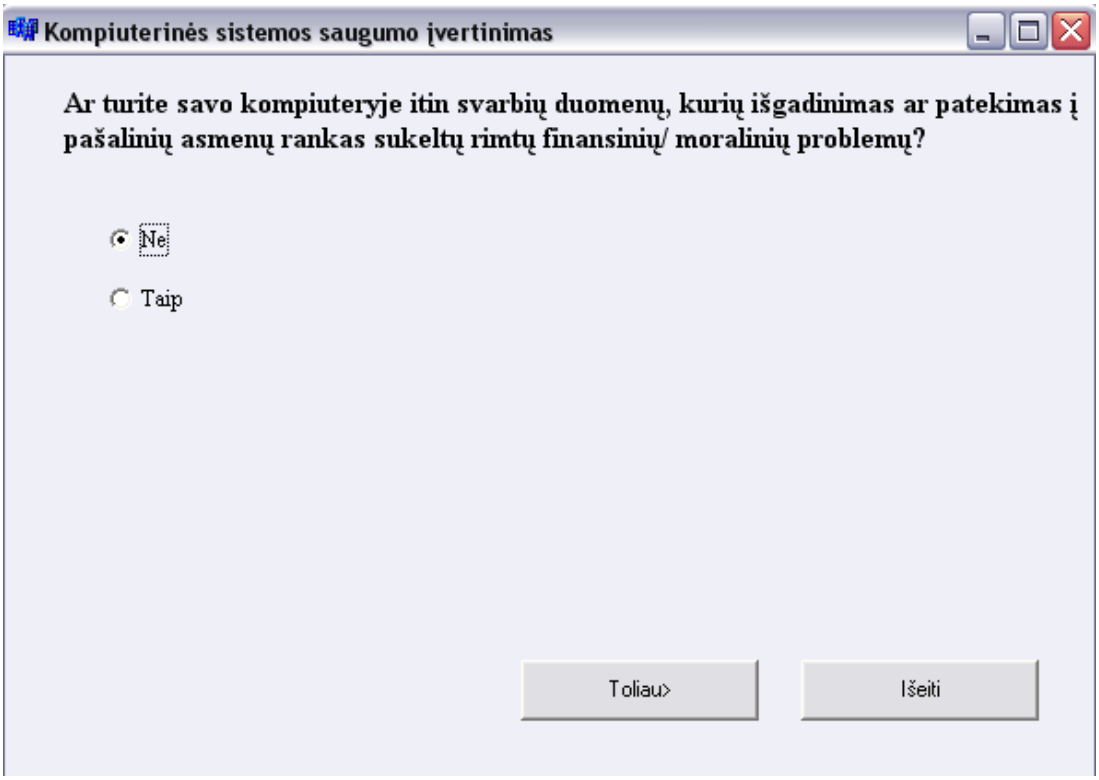
23 pav. Kompiuterio vartotojų patikimumo įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

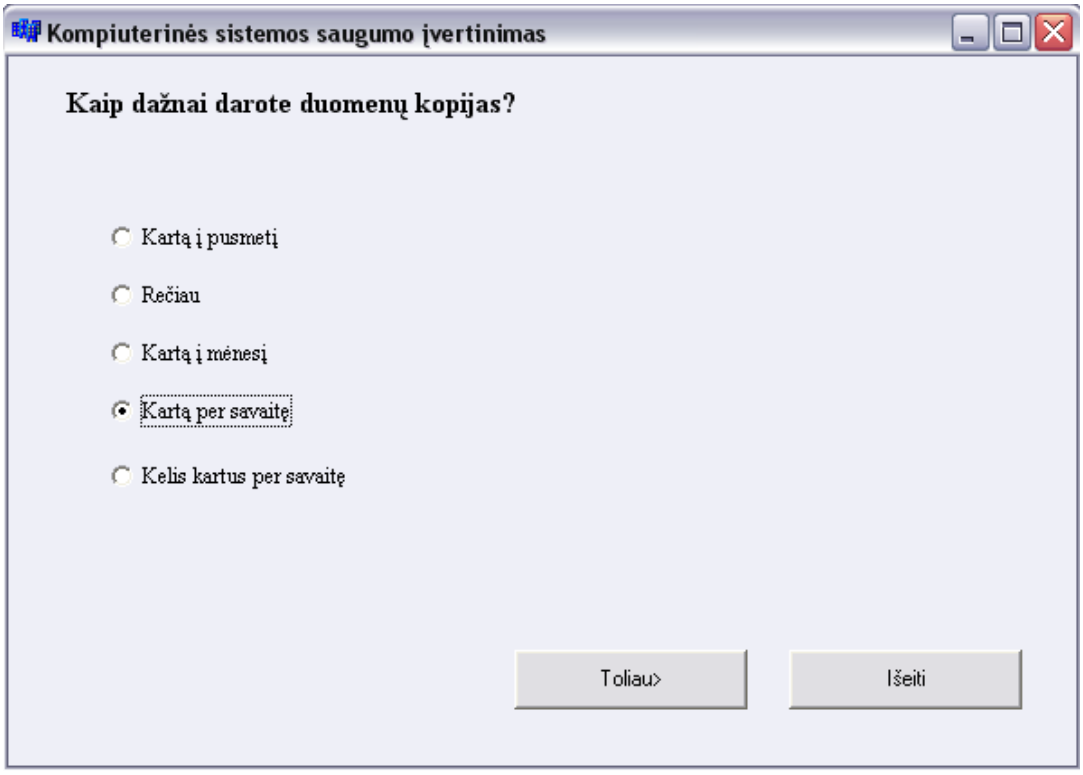
24 pav. Duomenų kopijų darymo įvertinimas



Šaltinis: sudaryta darbo autorės.

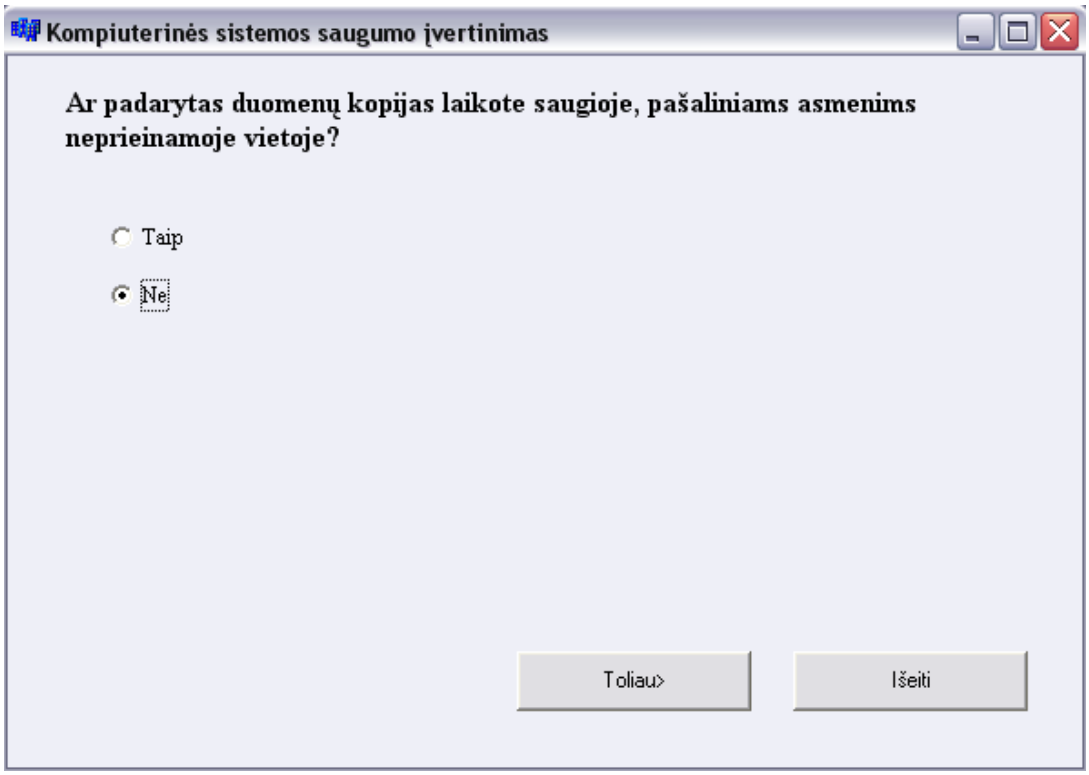
25 pav. Itin svarbių dokumentų būvimo įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

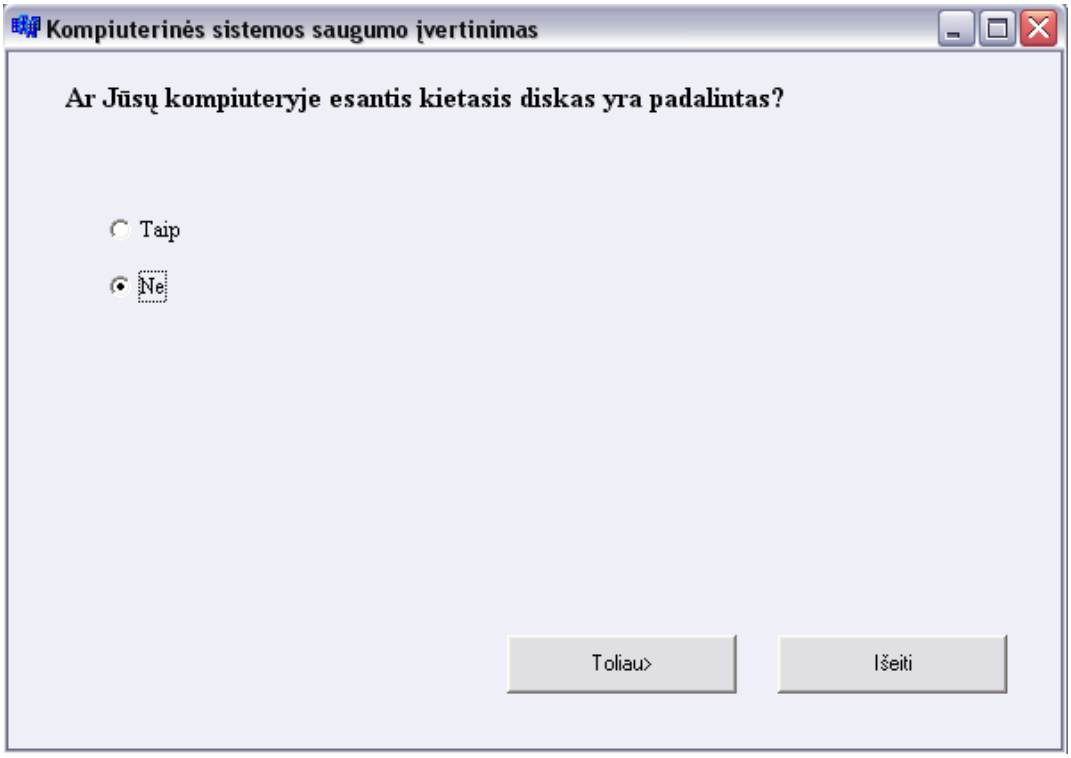
26 pav. Duomenų kopijų reguliaraus darymo įvertinimas



Šaltinis: sudaryta darbo autorės.

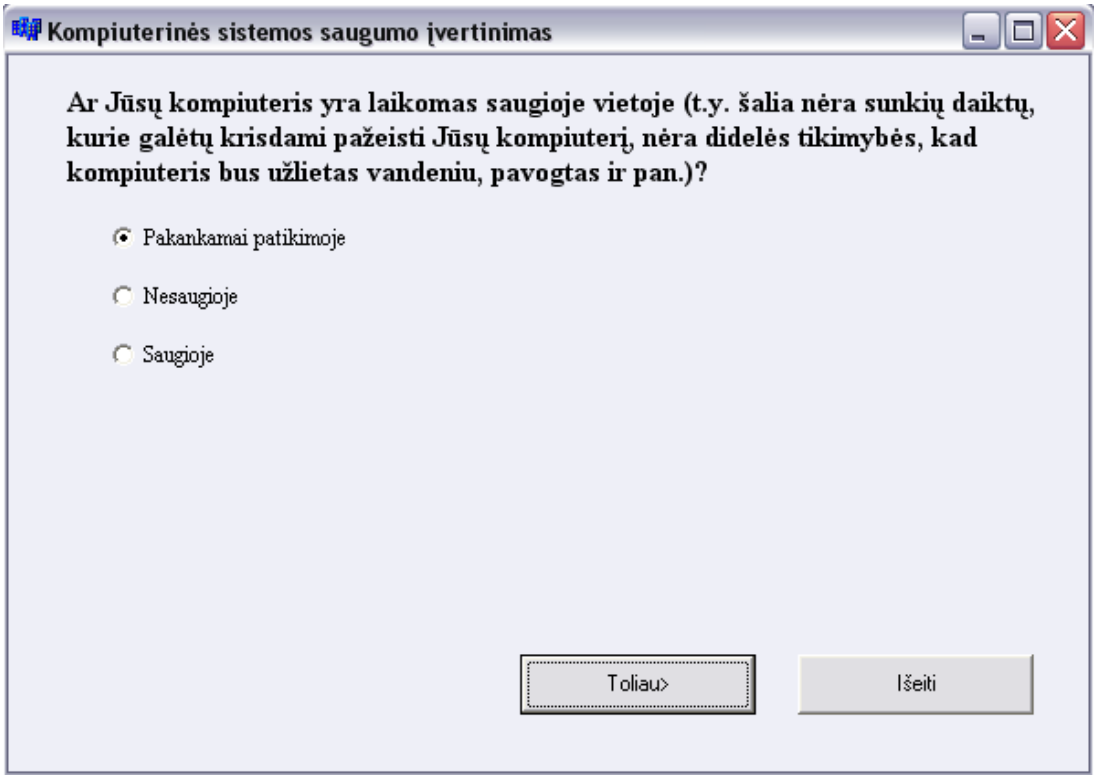
27 pav. Duomenų kopijų laikymo vietos įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

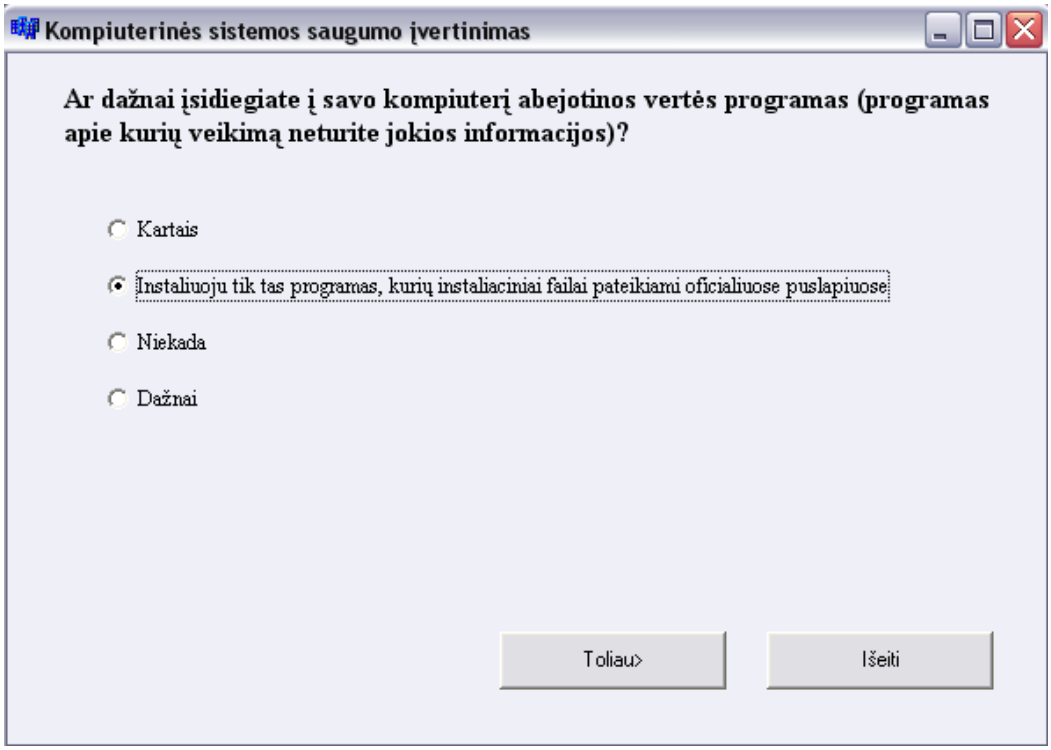
28 pav. Kompiuterio kietojo disko įvertinimas



Šaltinis: sudaryta darbo autorės.

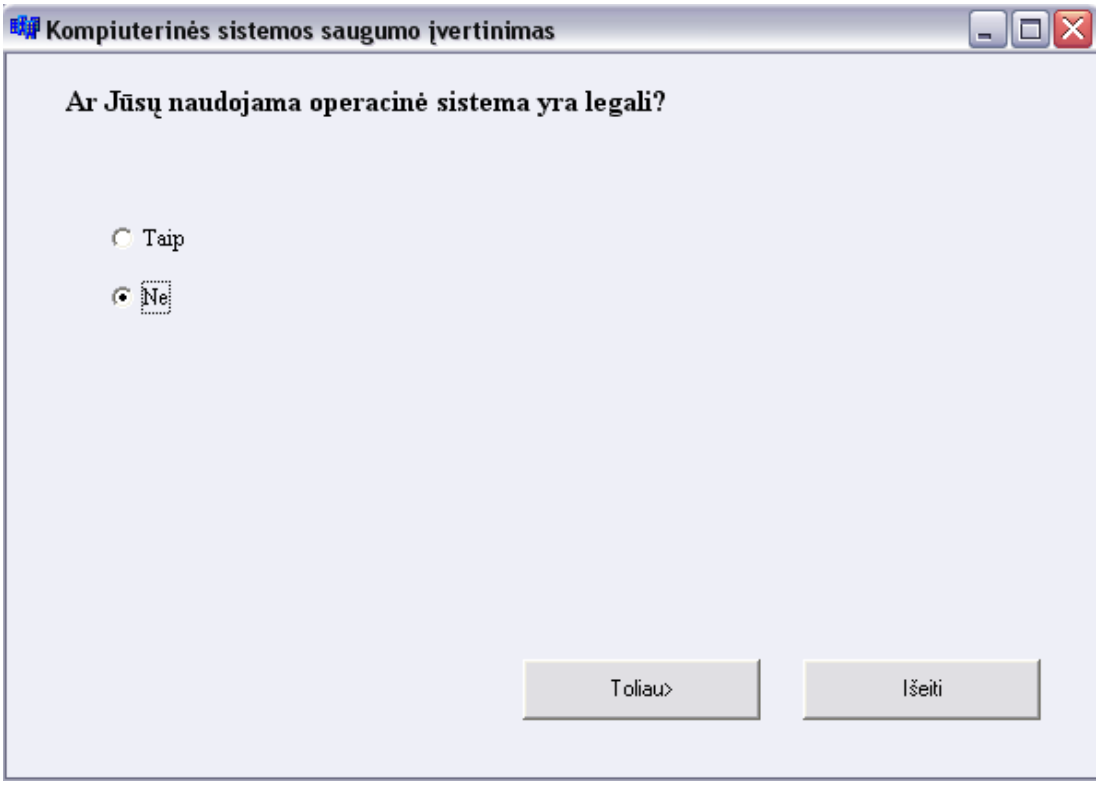
29 pav. Kompiuterio laikymo vietos įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

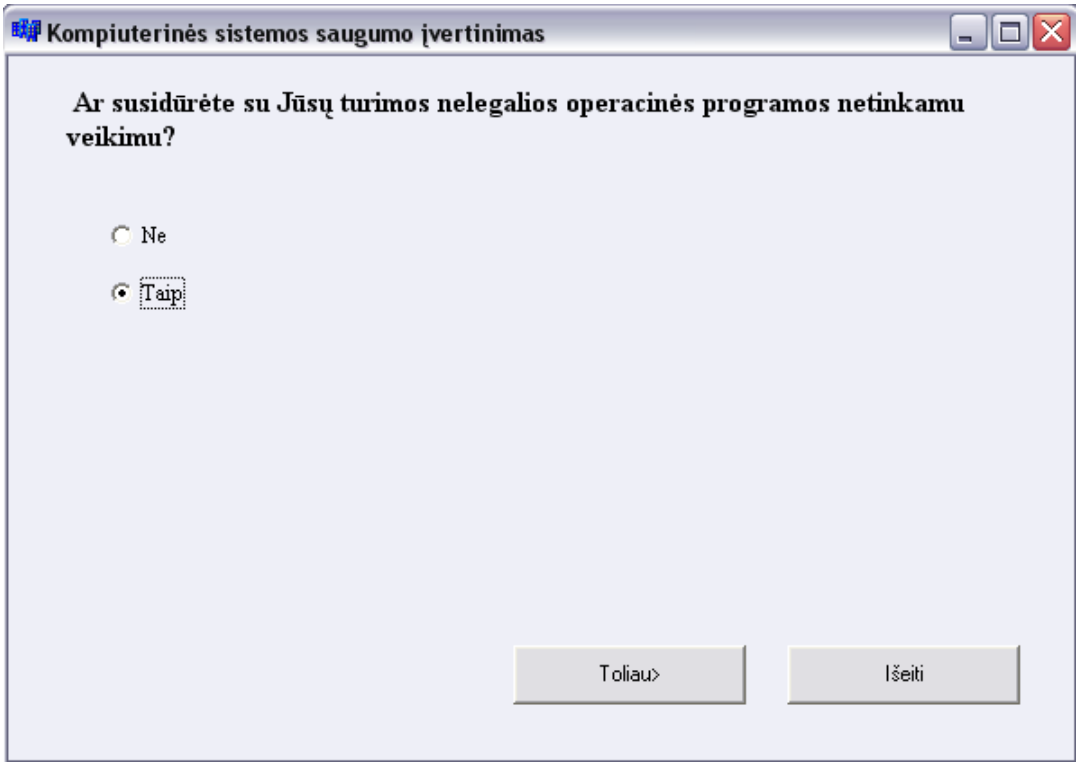
30 pav. Naudojimosi abejotinos vertės programomis įvertinimas



Šaltinis: sudaryta darbo autorės.

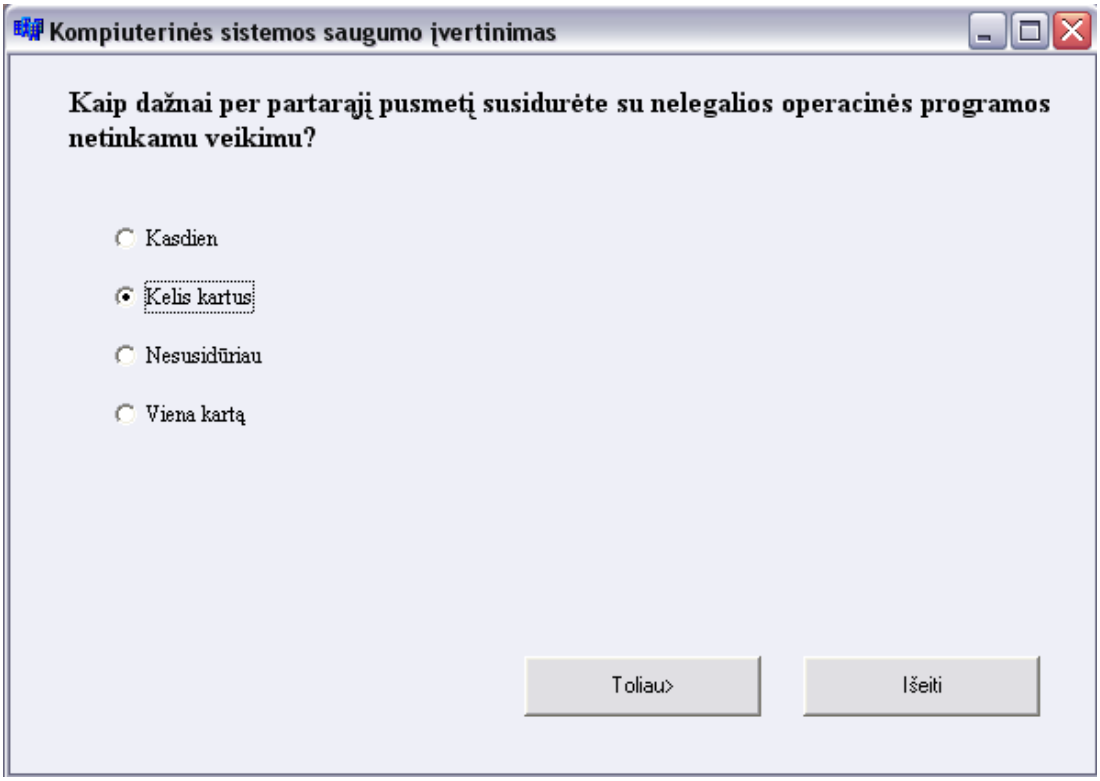
31 pav. Operacinės sistemos legalumo įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

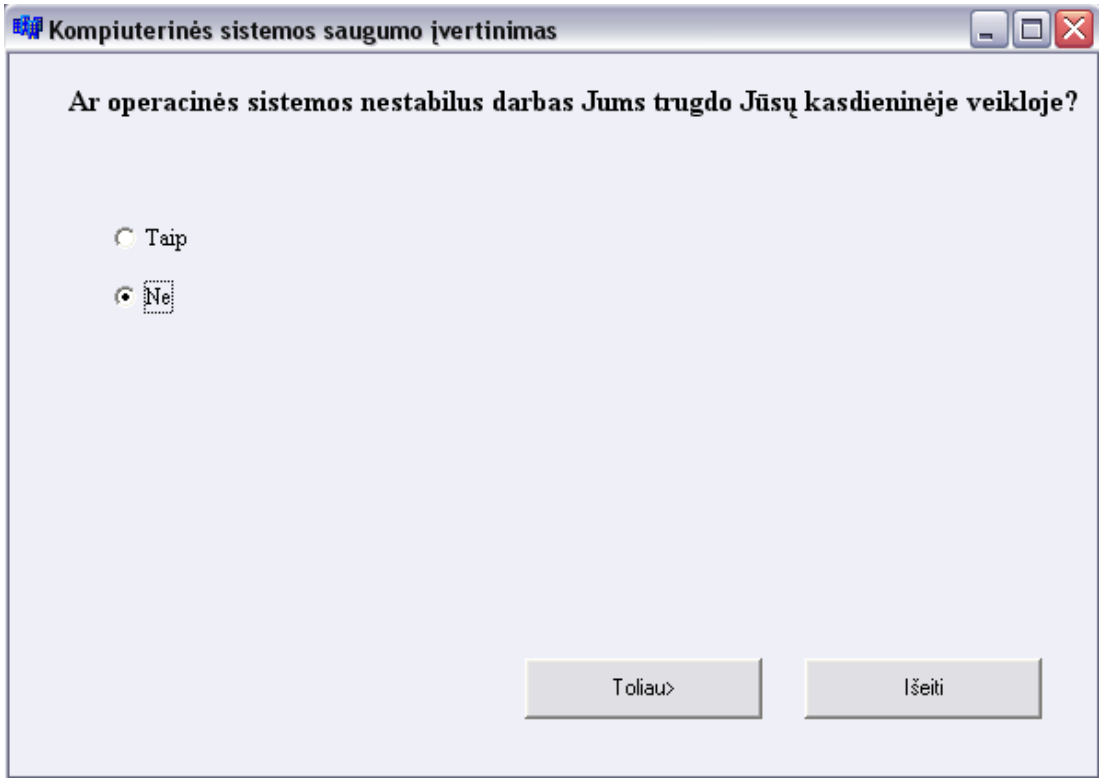
32 pav. Nelegalios operacinės sistemos veikimo įvertinimas



Šaltinis: sudaryta darbo autorės.

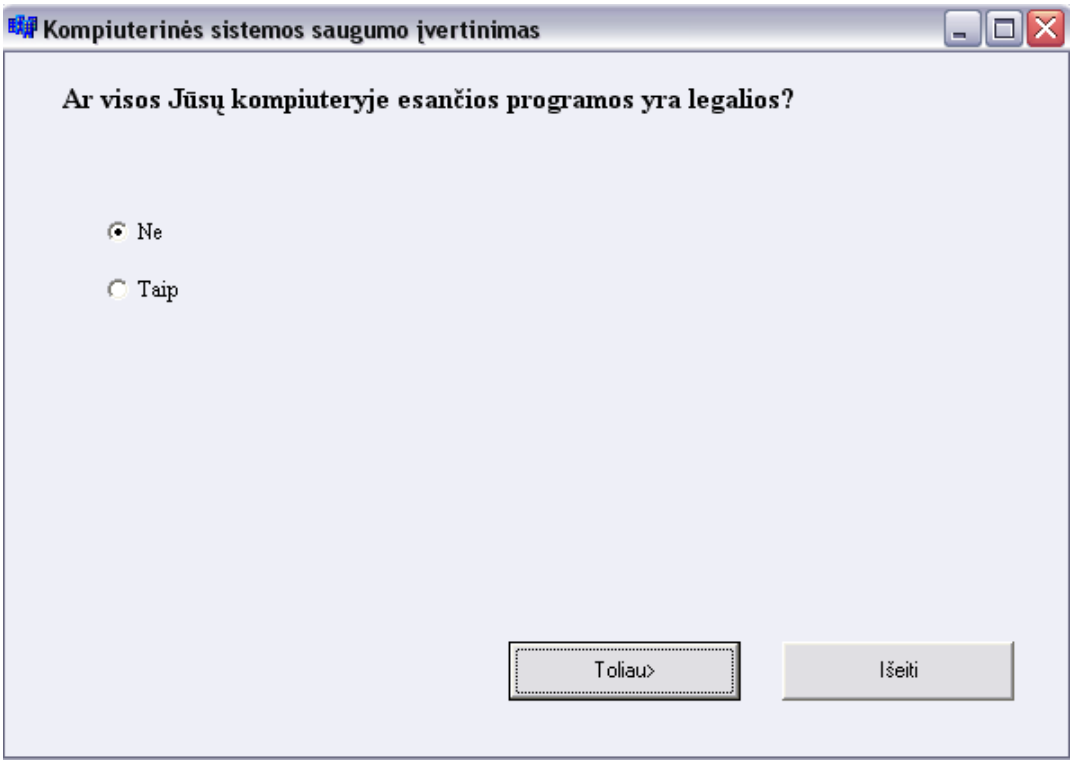
33 pav. Nelegalios operacinės sistemos netinkamo veikimo įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

34 pav. Nelegalios operacinės sistemos poveikio kasdieninėje veikloje įvertinimas



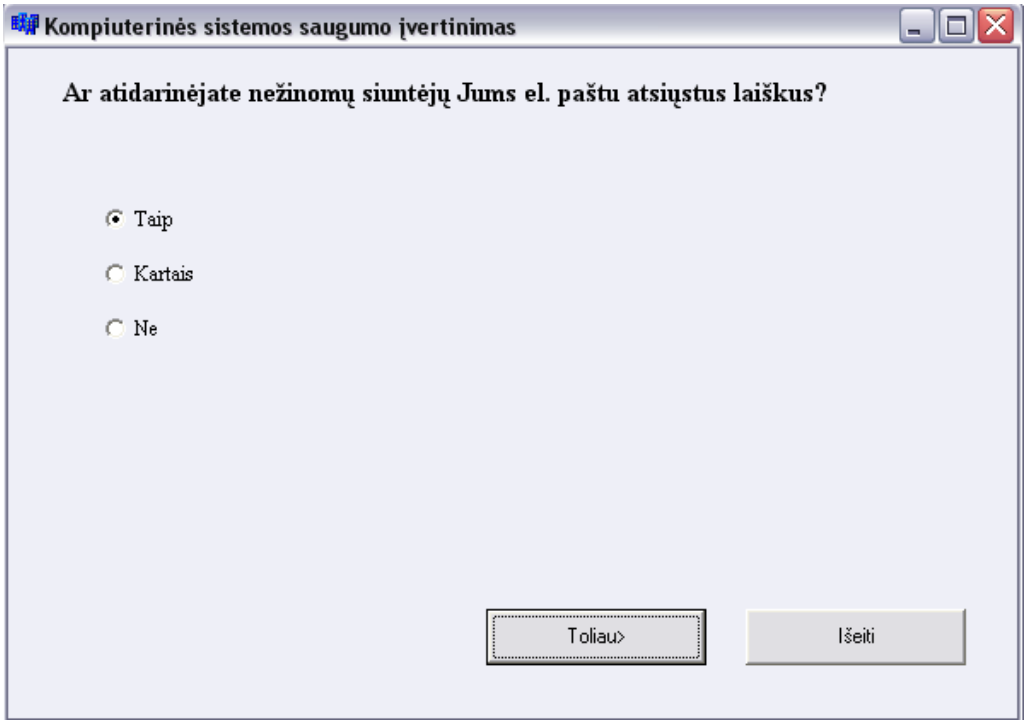
Šaltinis: sudaryta darbo autorės.

35 pav. Programų legalumo įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai

Šaltinis: sudaryta darbo autorės.

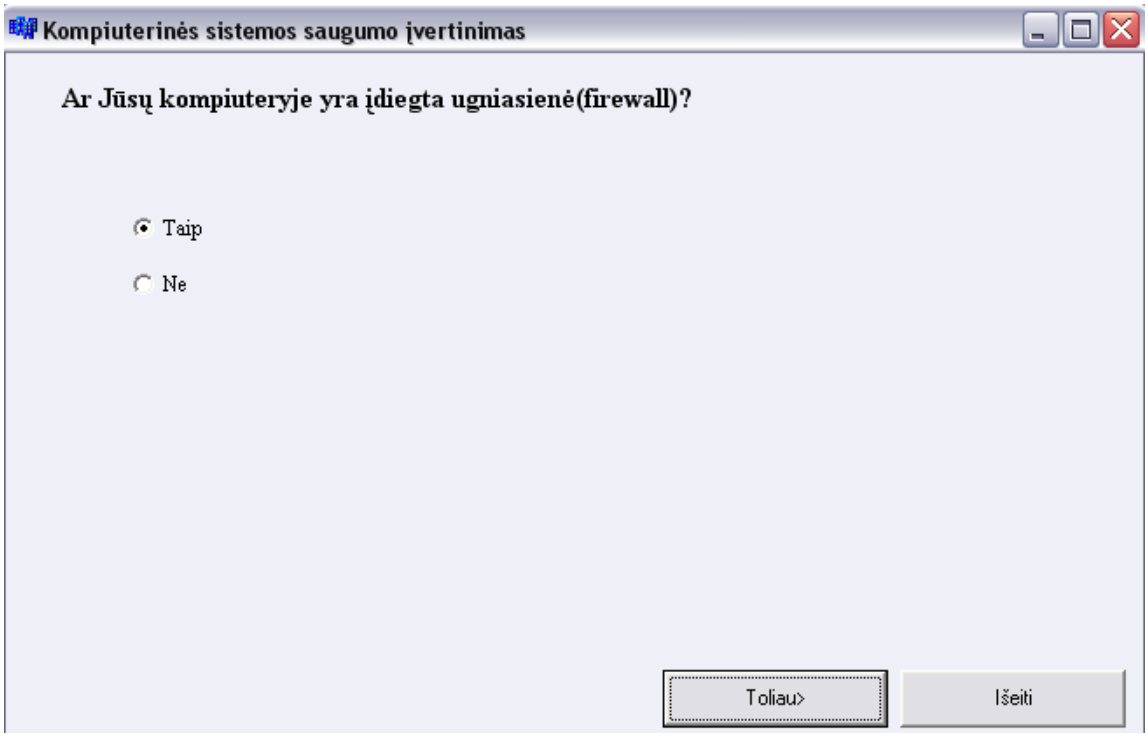
36 pav. Naudojimosi elektroniniu paštu įvertinimas



Šaltinis: sudaryta darbo autorės.

37 pav. Nežinomų laiškų atidarinėjimo dažnumo įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



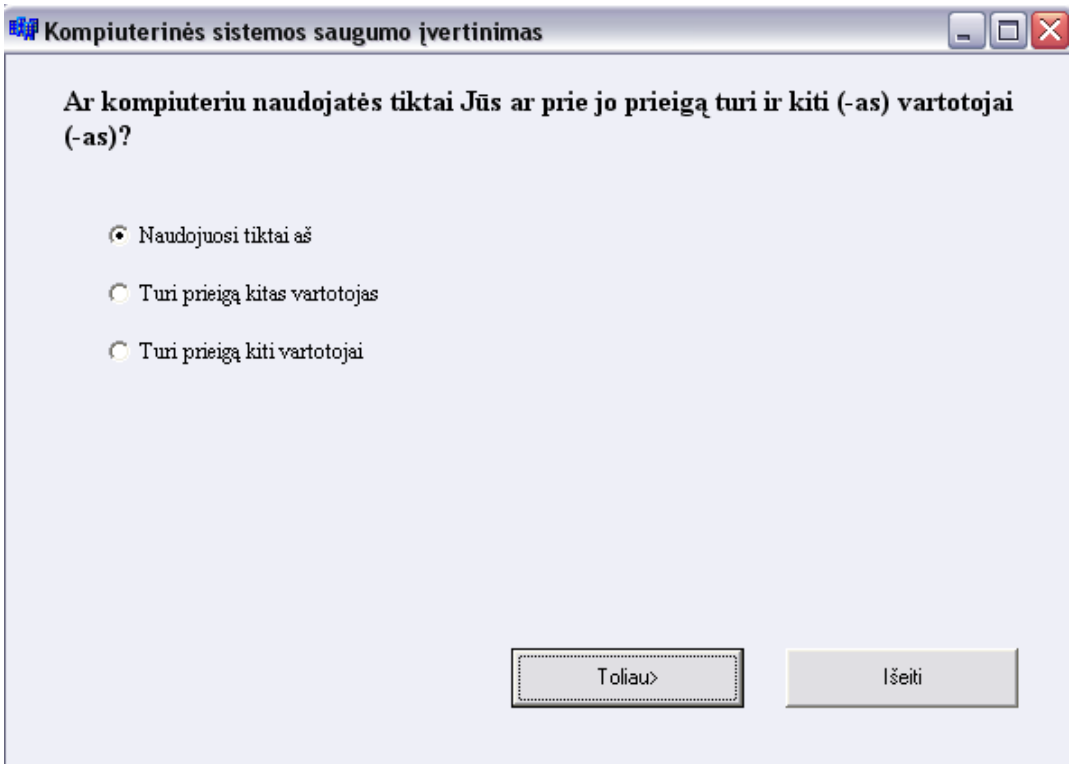
Šaltinis: sudaryta darbo autorės.

38 pav. Ugniasienės buvimo įvertinimas

Šaltinis: sudaryta darbo autorės.

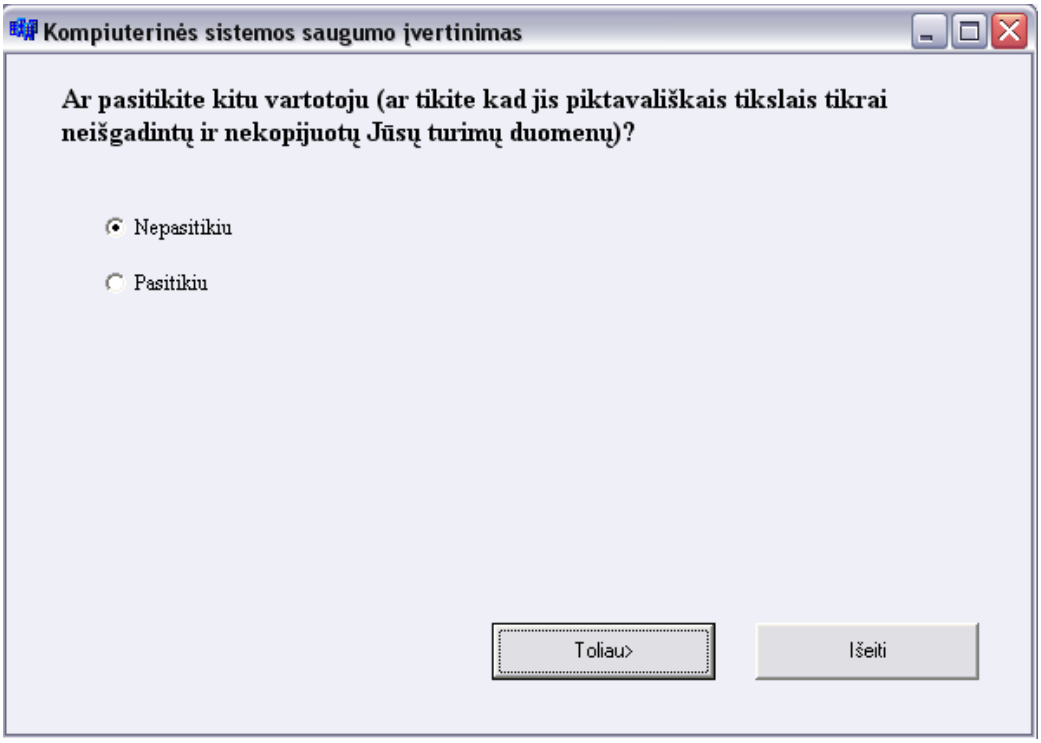
39 pav. Virusų padarytos žalos įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

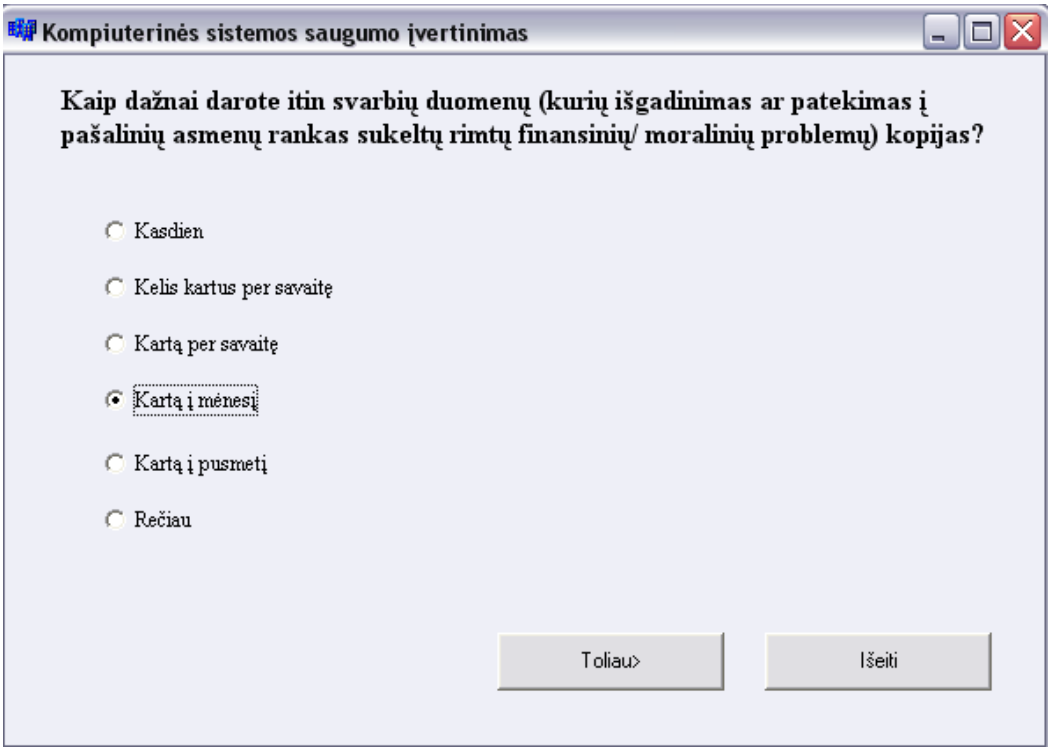
40 pav. Vartotojų dirbančių su kompiuteriu įvertinimas



Šaltinis: sudaryta darbo autorės.

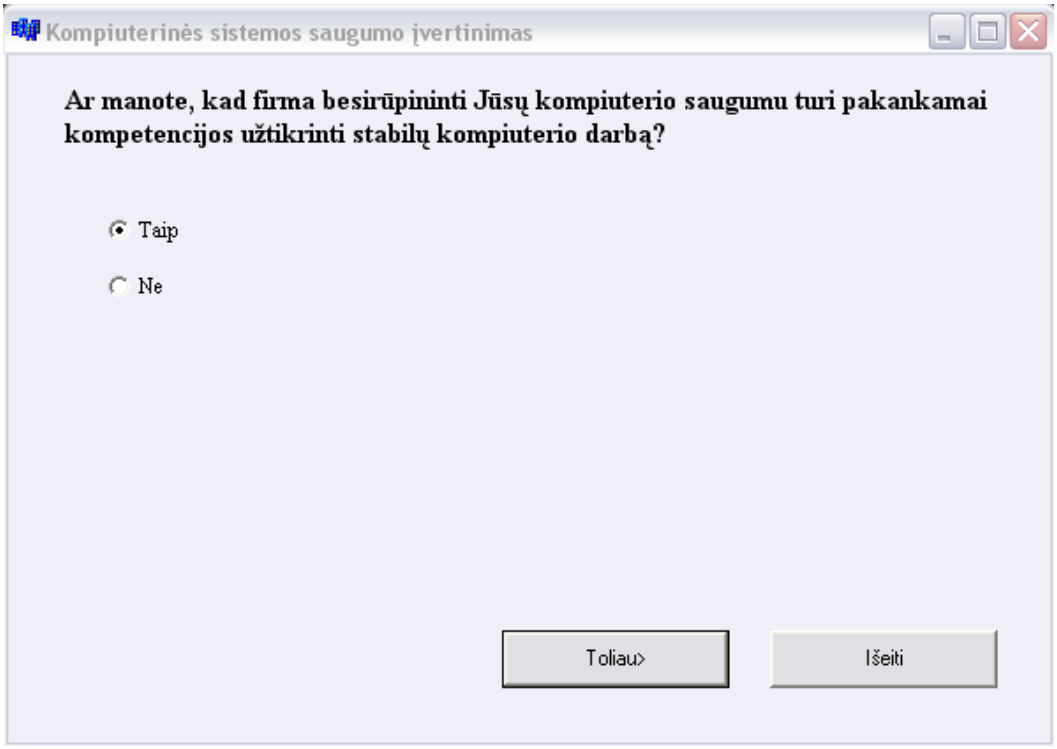
41 pav. Pasitikėjimo kompiuterio vartotoju įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

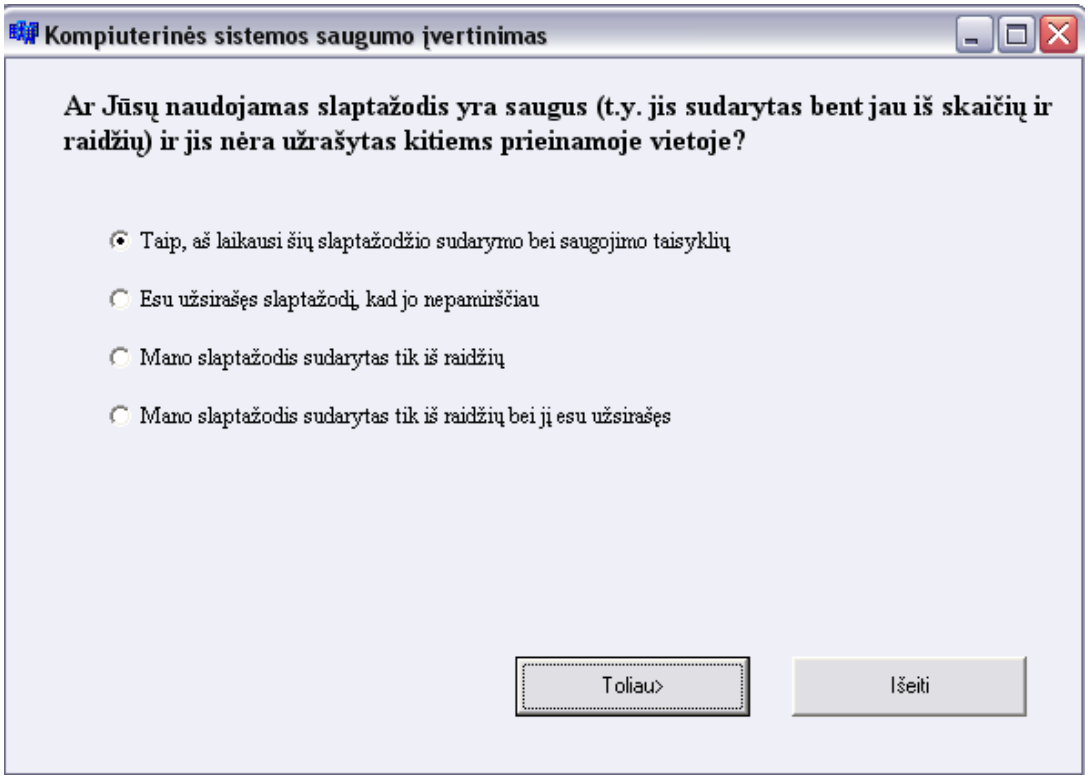
42 pav. Itin svarbių dokumentų kopijų darymo reguliarumo įvertinimas



Šaltinis: sudaryta darbo autorės.

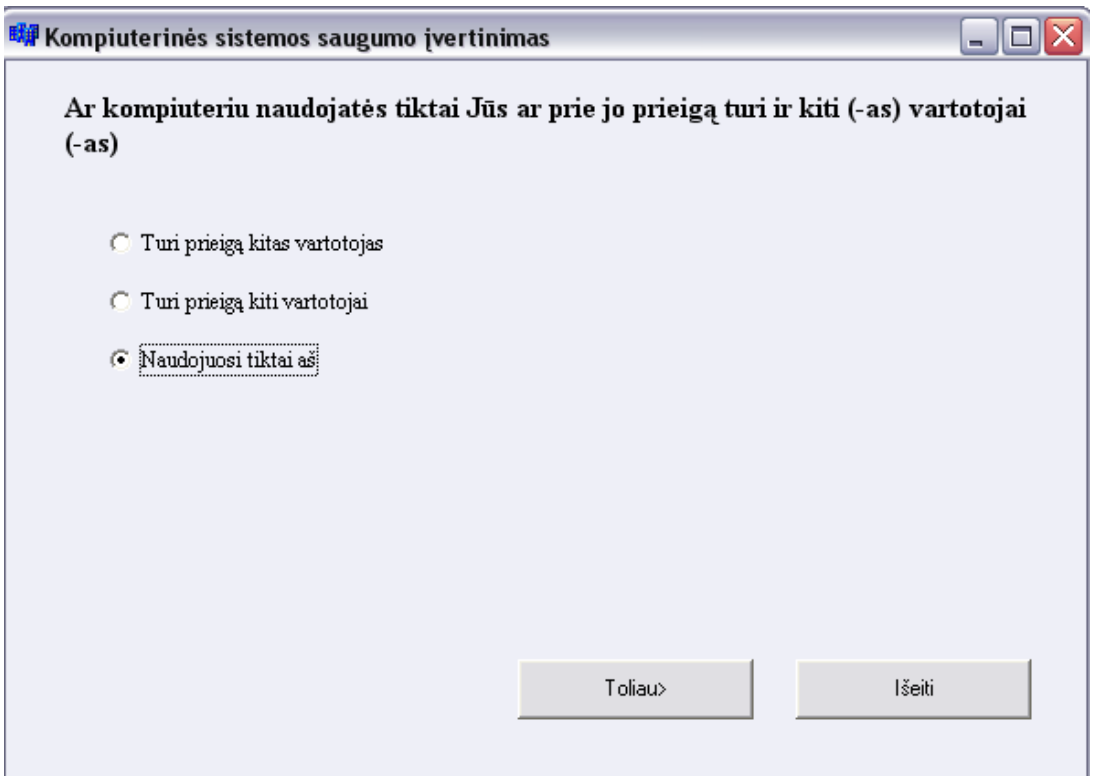
43 pav. Firmos besirūpinančios kompiuteriu saugumu kompetencijos įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

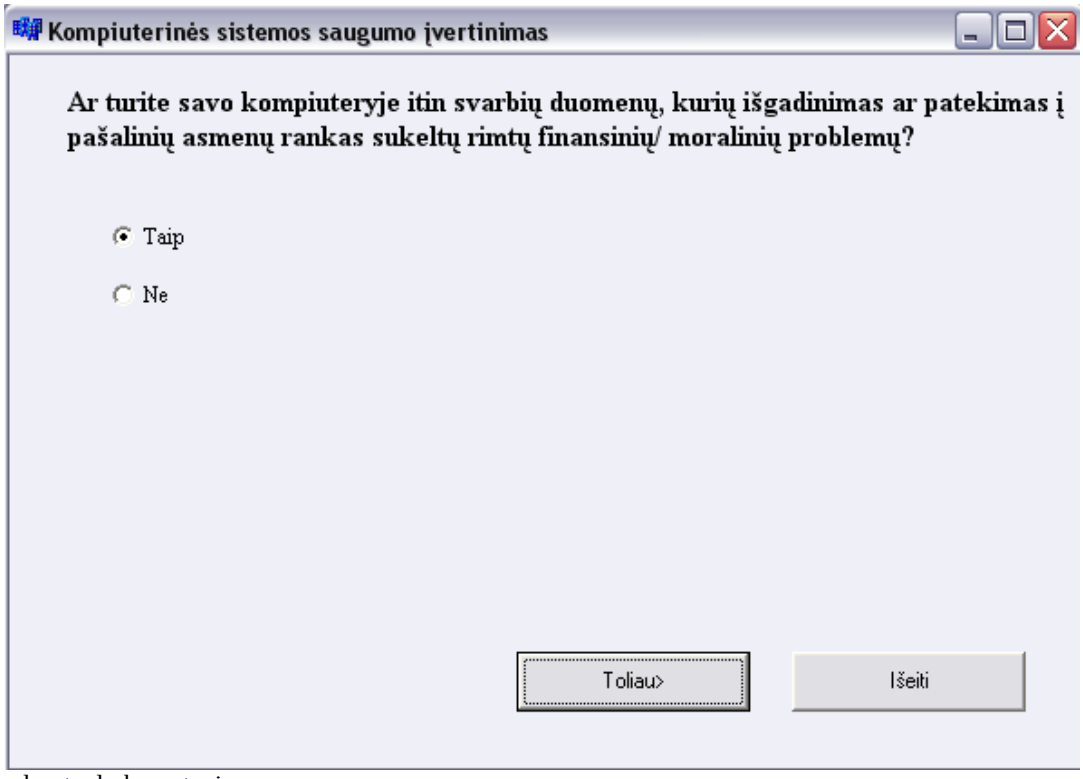
44 pav. Naudojamo slaptažodžio saugumo įvertinimas



Šaltinis: sudaryta darbo autorės.

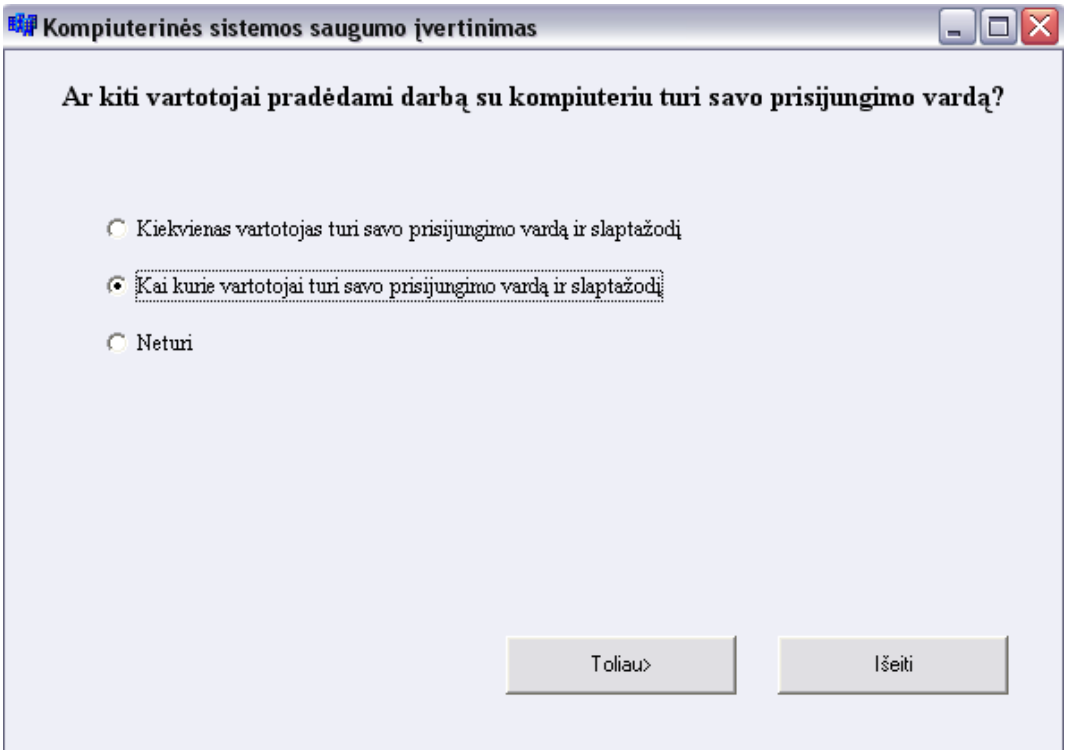
45 pav. Kompiuterio vartotojų skaičiaus įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

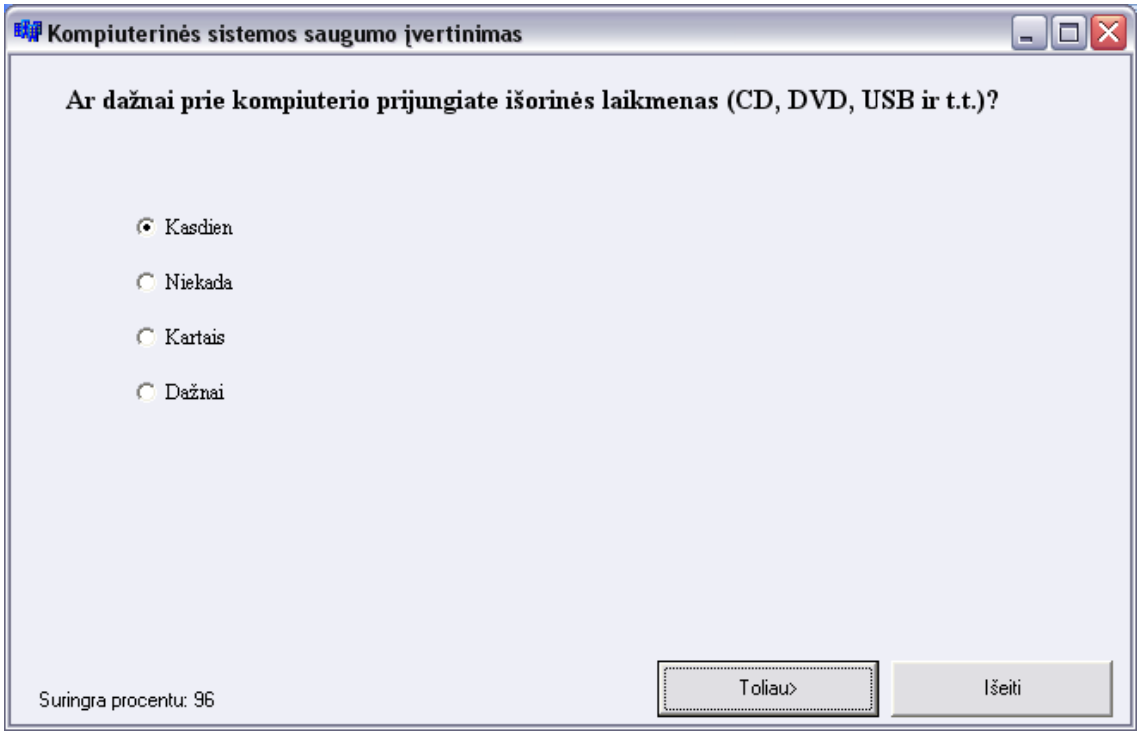
46 pav. Itin svarbių dokumentų kompiuteryje būvimo įvertinimas



Šaltinis: sudaryta darbo autorės.

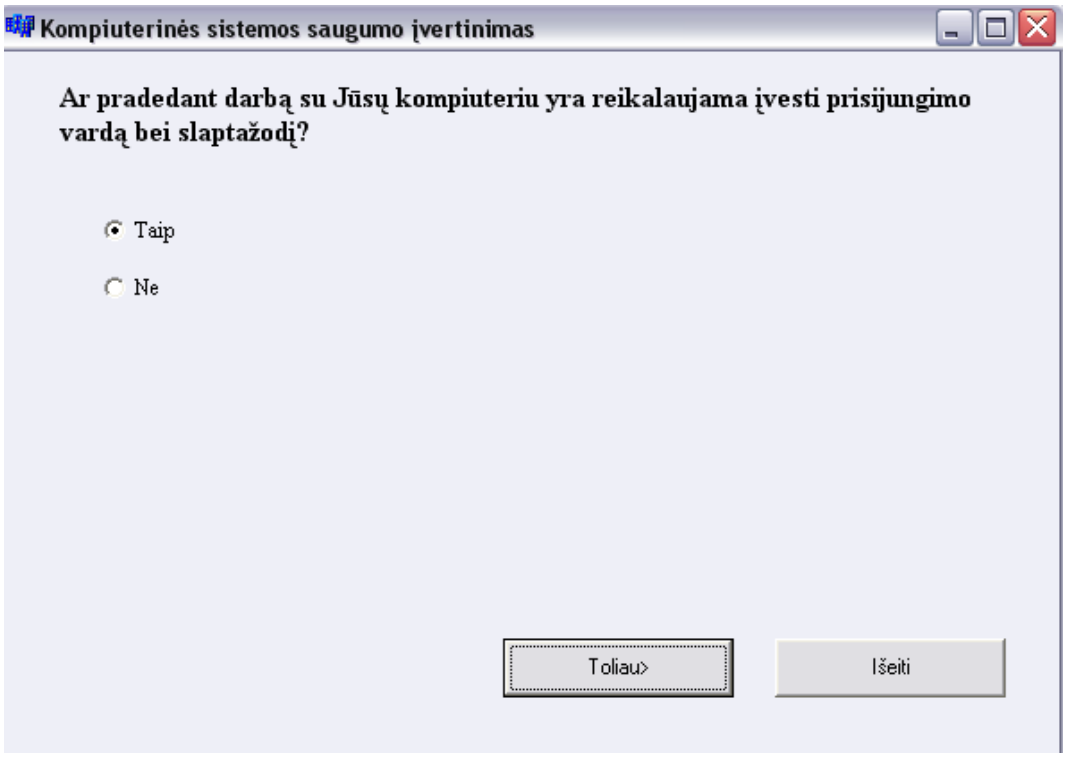
47 pav. Vartotojų prisijungimo vardų bei slaptažodžių būvimo įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

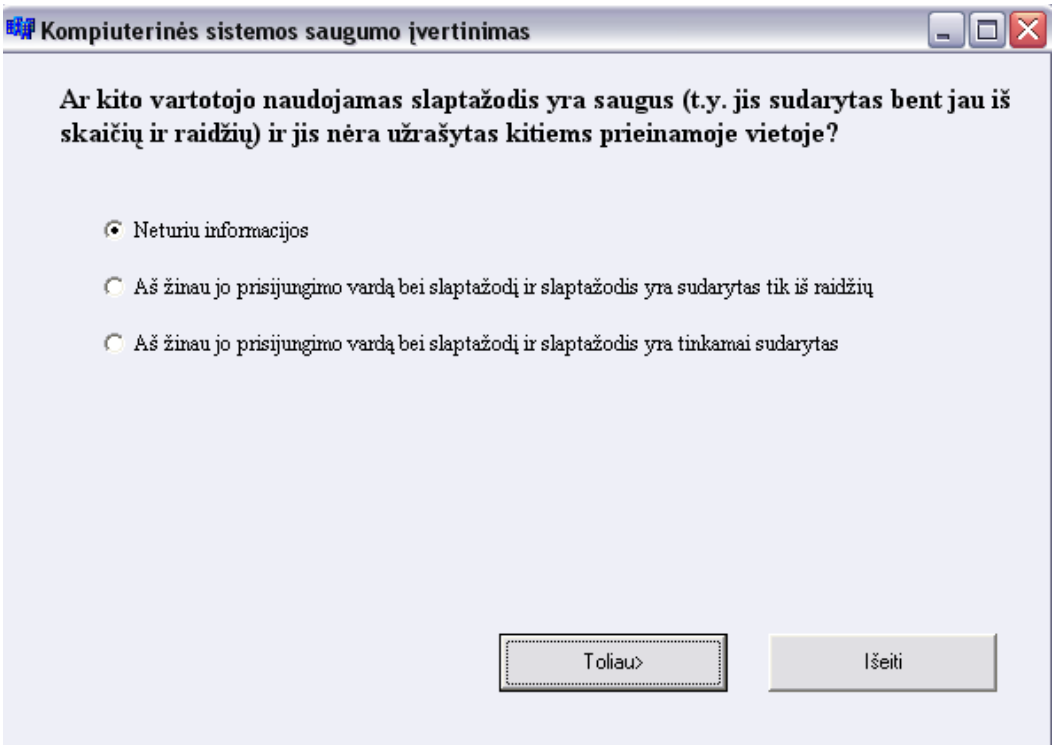
48 pav. Papildomų informacijos laikmenų prijungimo prie kompiuterio dažnumo įvertinimas



Šaltinis: sudaryta darbo autorės.

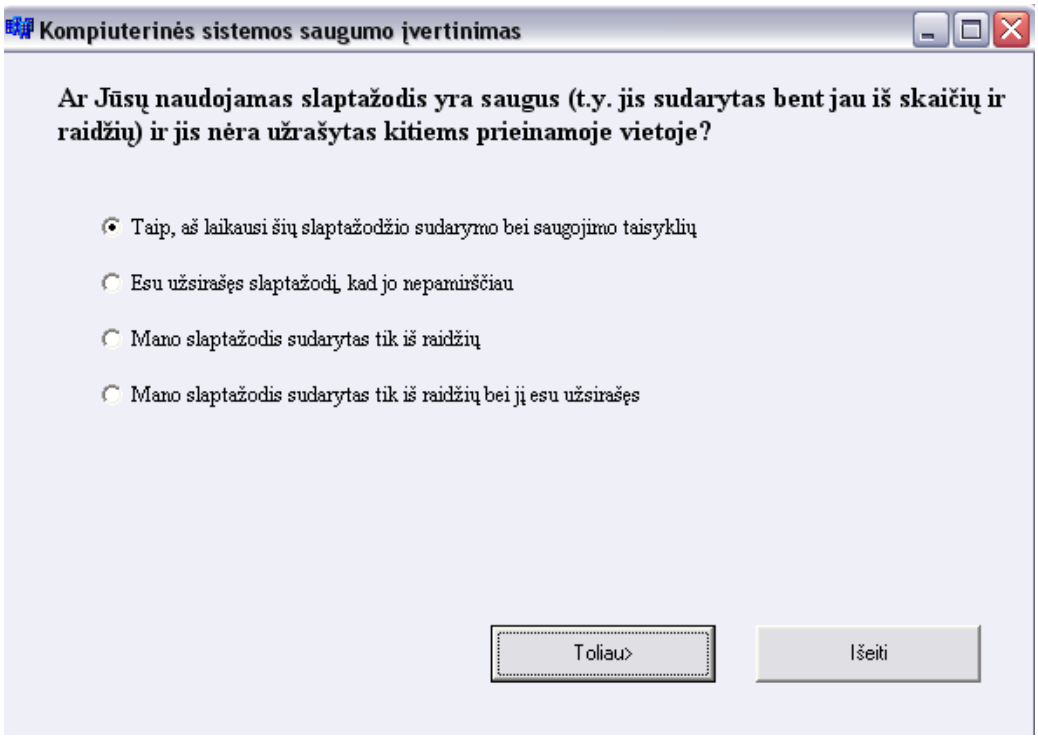
49 pav. Slaptažodžio būvimo įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

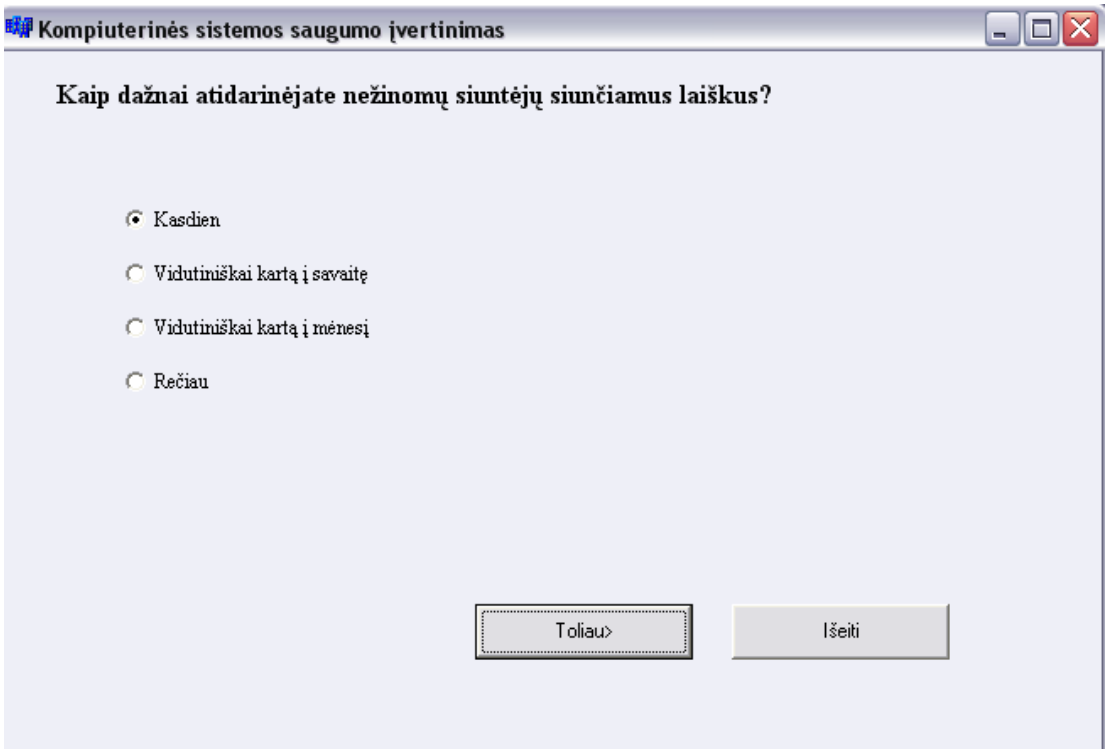
50 pav. Antrojo vartotojo slaptažodžio patikimumo įvertinimas



Šaltinis: sudaryta darbo autorės.

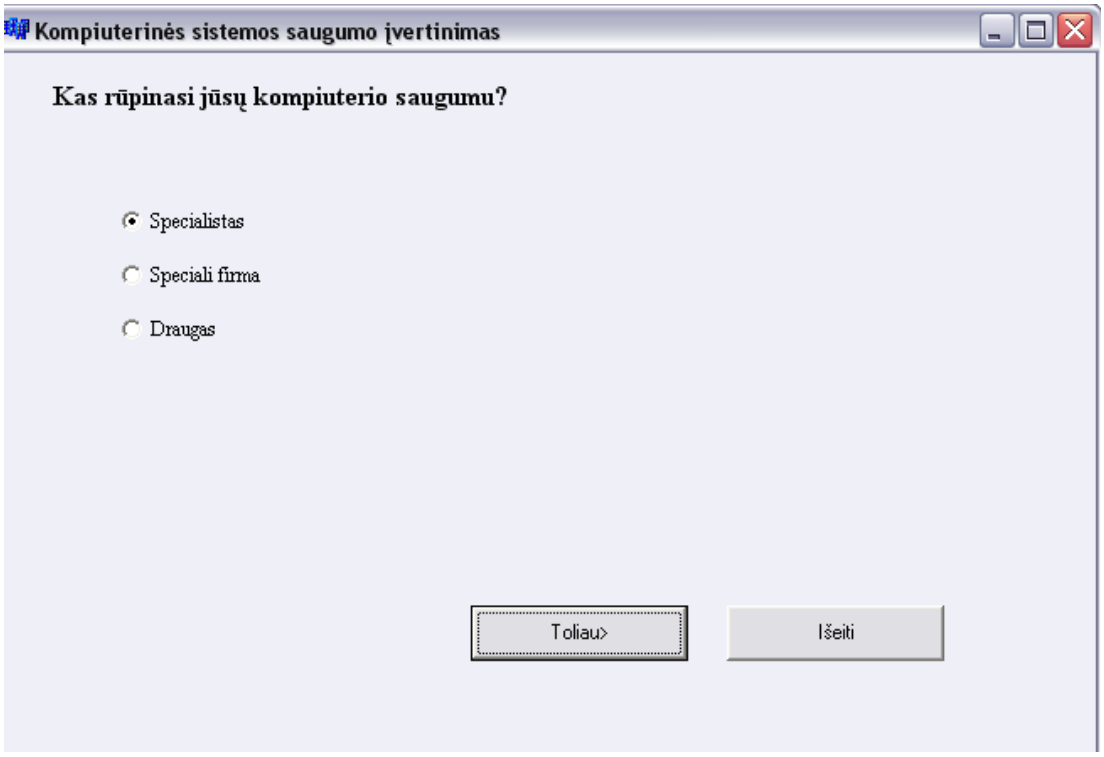
51 pav. Vartotojo slaptažodžio patikimumo įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

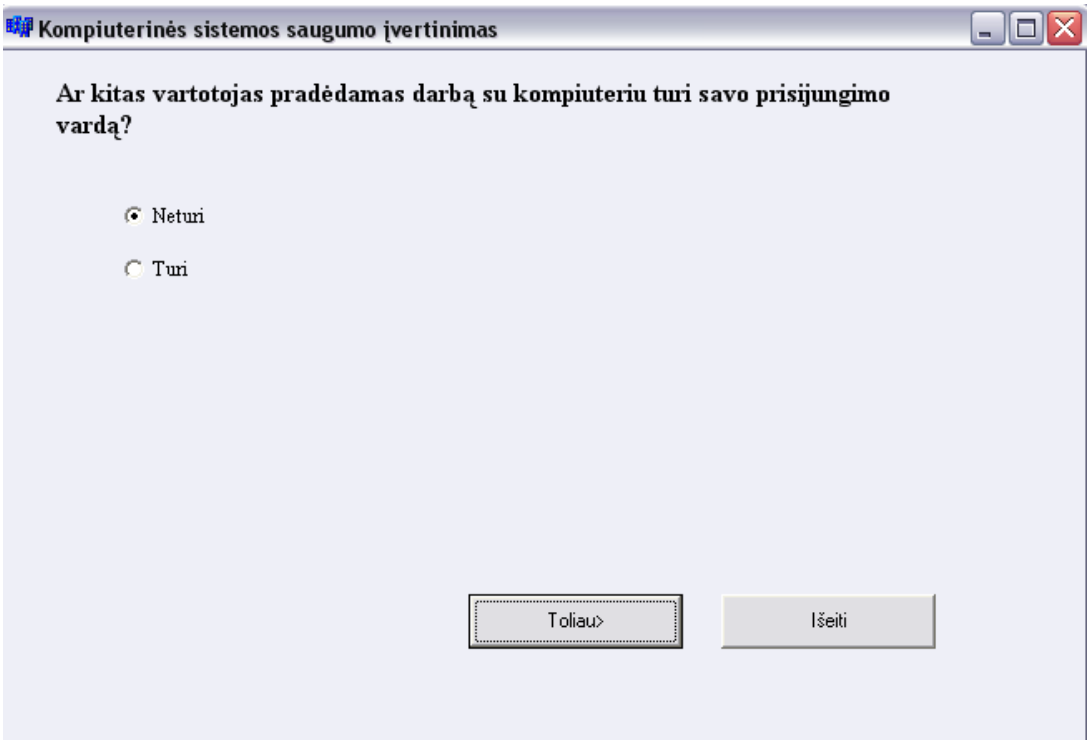
52 pav. Nežinomų laiškų atidarinėjimo dažnumo įvertinimas



Šaltinis: sudaryta darbo autorės.

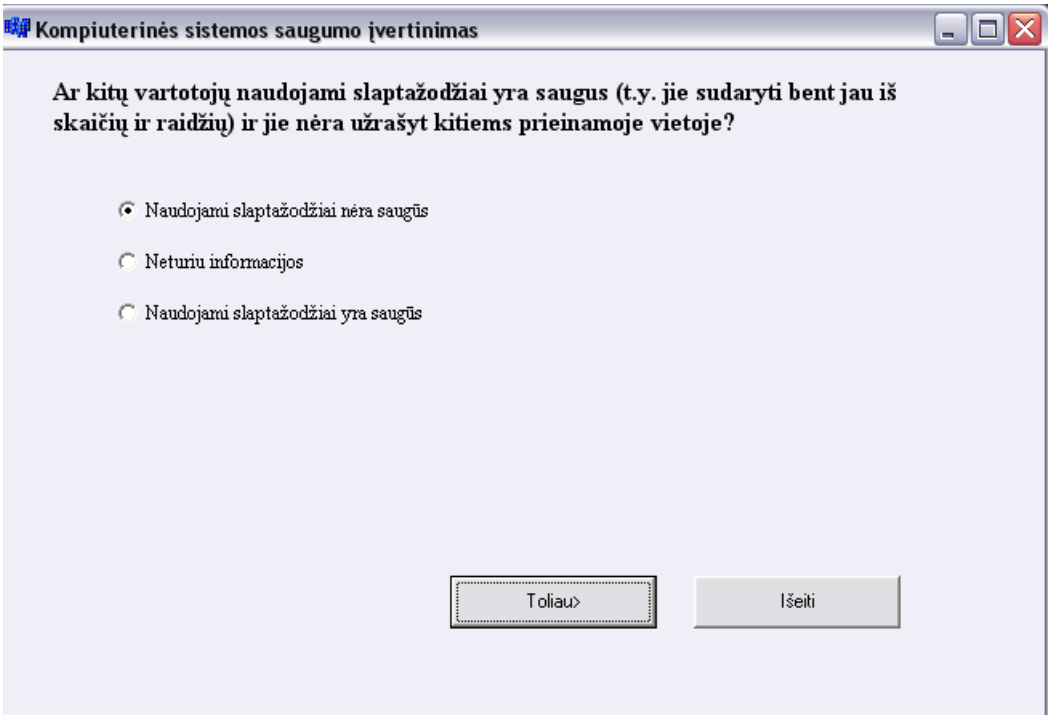
53 pav. Kompiuterio saugumu besirūpinančio asmens išsiaiškinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

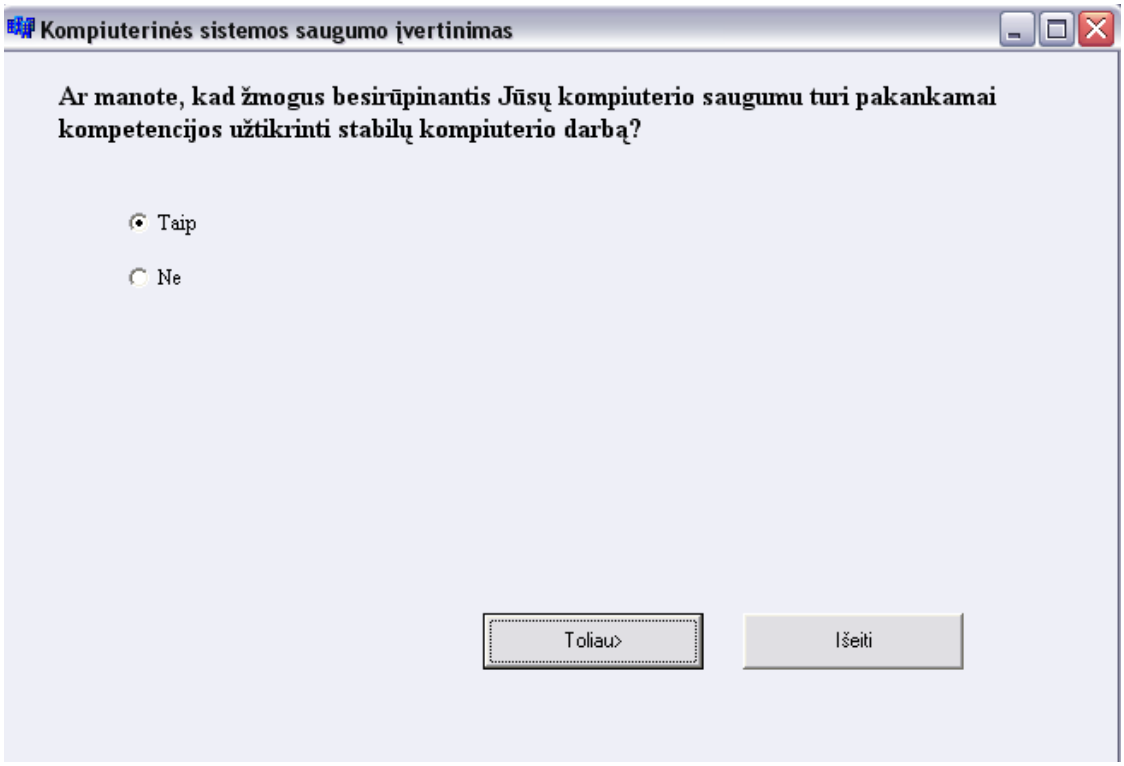
54 pav. Slaptažodžio būvimo įvertinimas



Šaltinis: sudaryta darbo autorės.

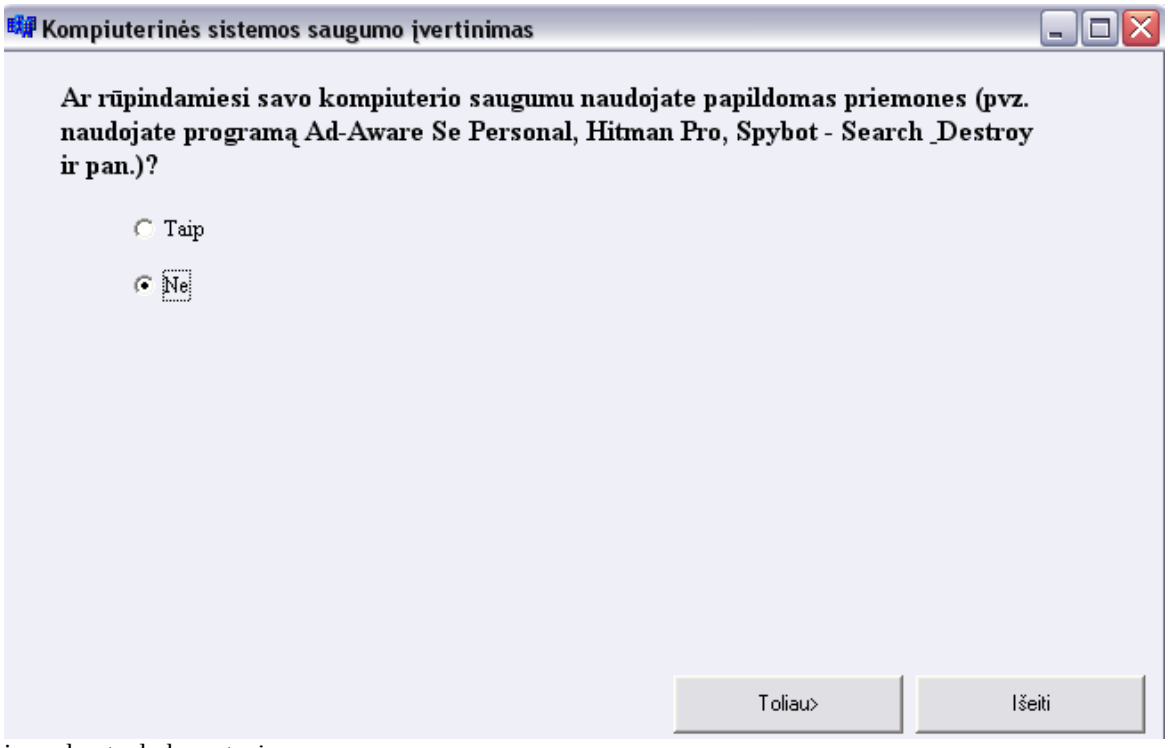
55 pav. Slaptažodžių saugumo įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

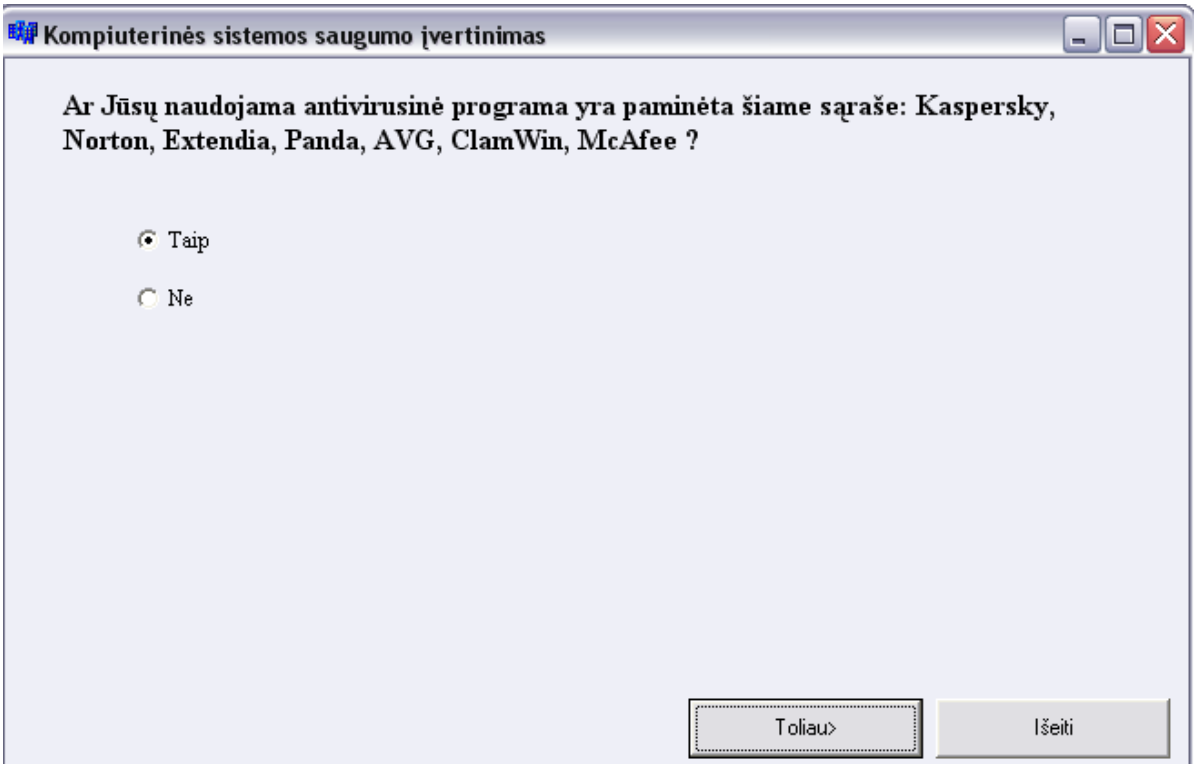
56 pav. Kompiuterių priežiūros specialisto kompetencijos įvertinimas



Šaltinis: sudaryta darbo autorės.

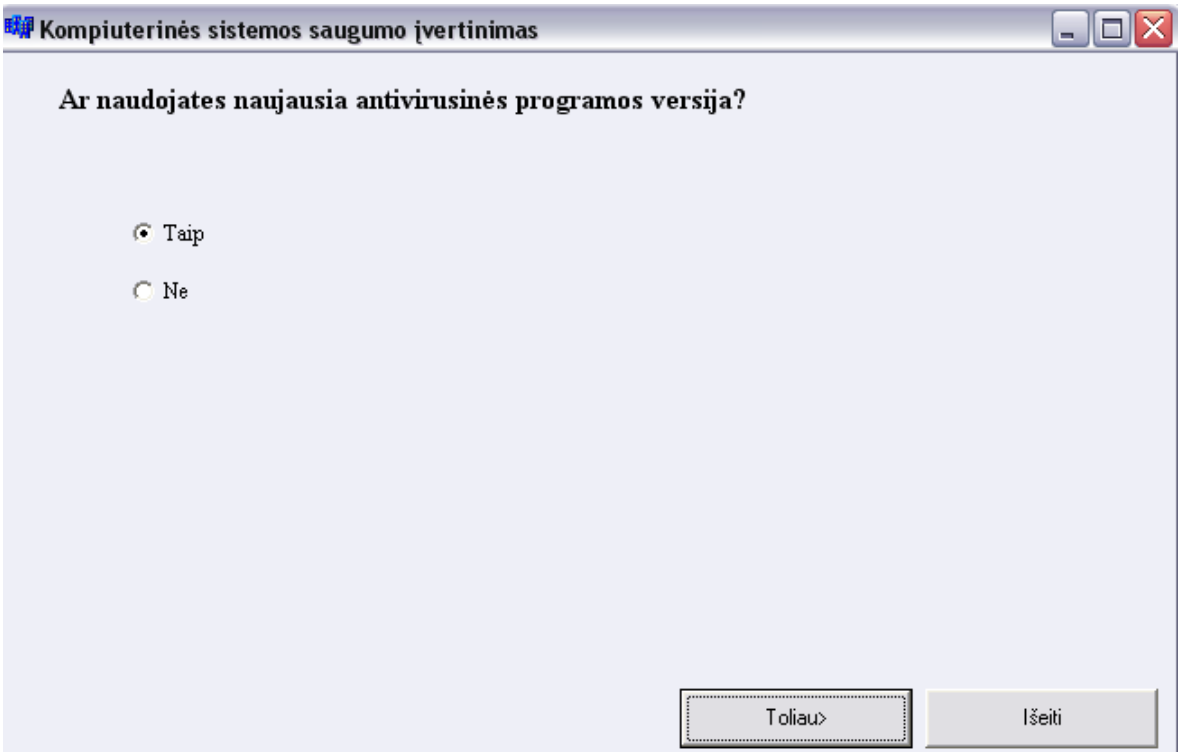
57pav. Slaptažodžio saugumo nustatymas su specialia programa

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

58 pav. Antivirusinės sistemos įvertinimas



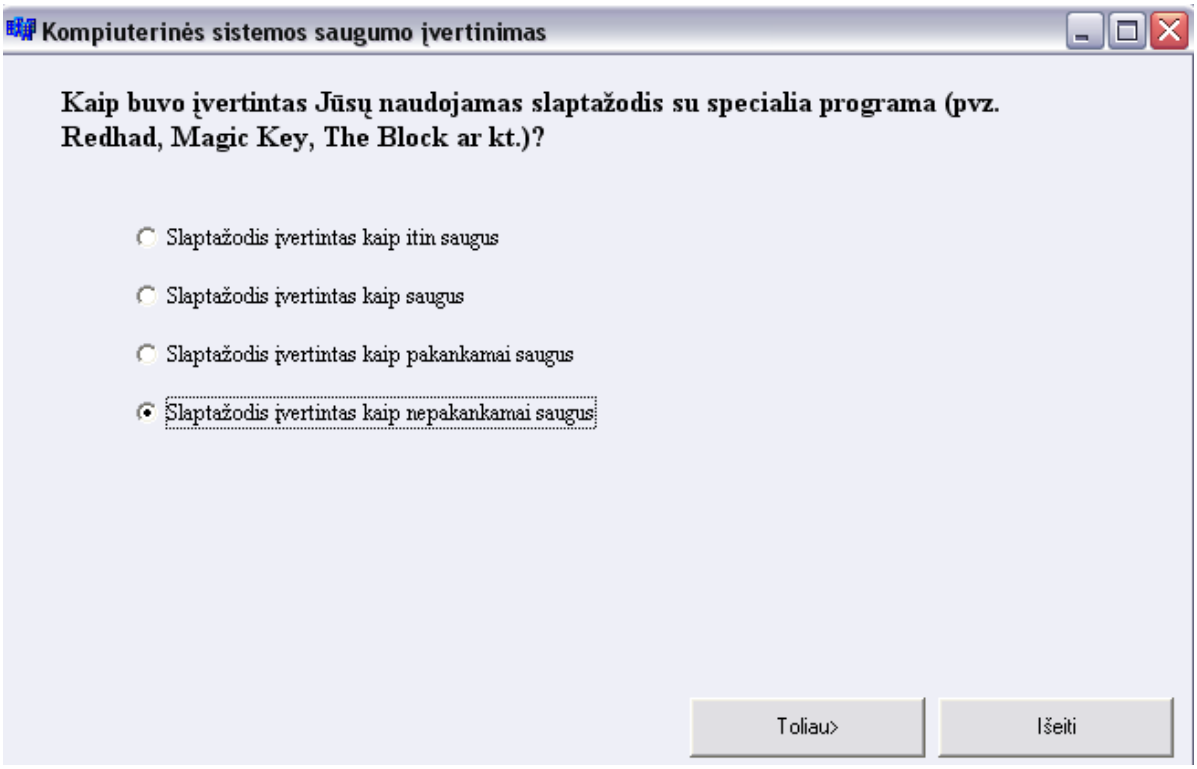
Šaltinis: sudaryta darbo autorės.

59 pav. Antivirusinės sistemos versijos įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai

Šaltinis: sudaryta darbo autorės.

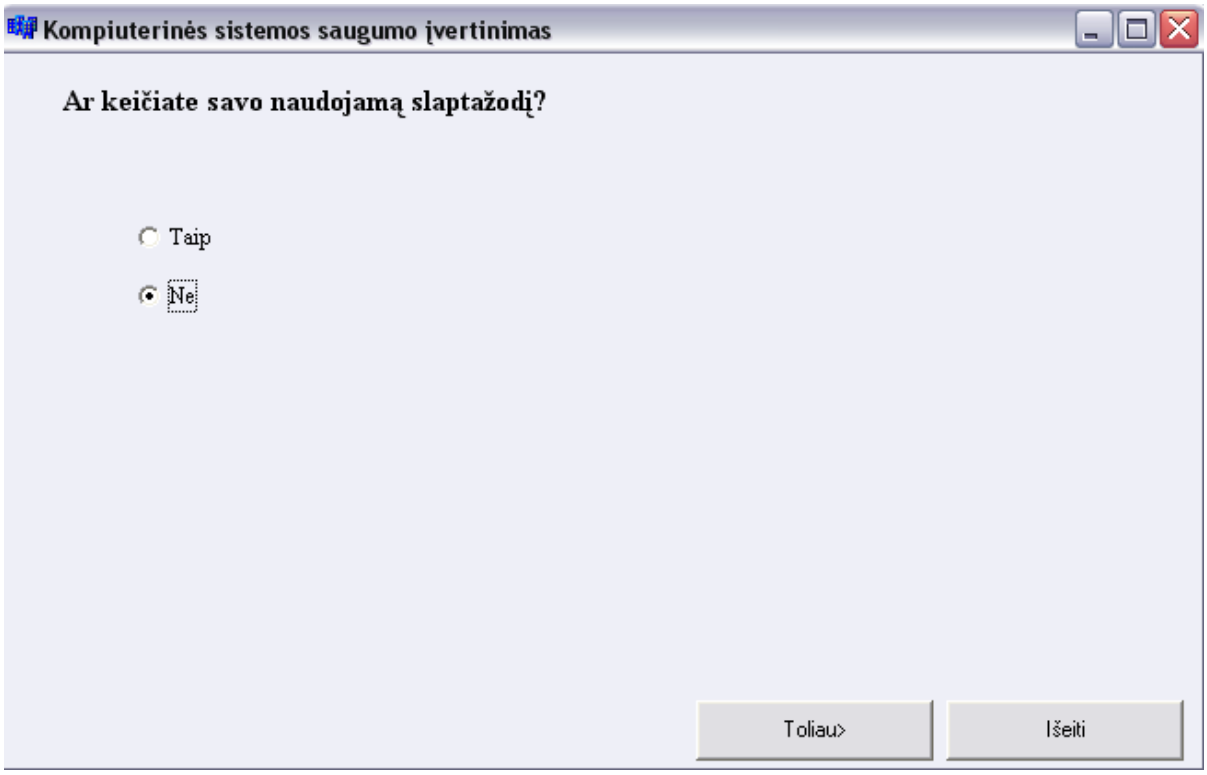
60 pav. Slaptažodžių saugumo įvertinimas su specialia programa



Šaltinis: sudaryta darbo autorės.

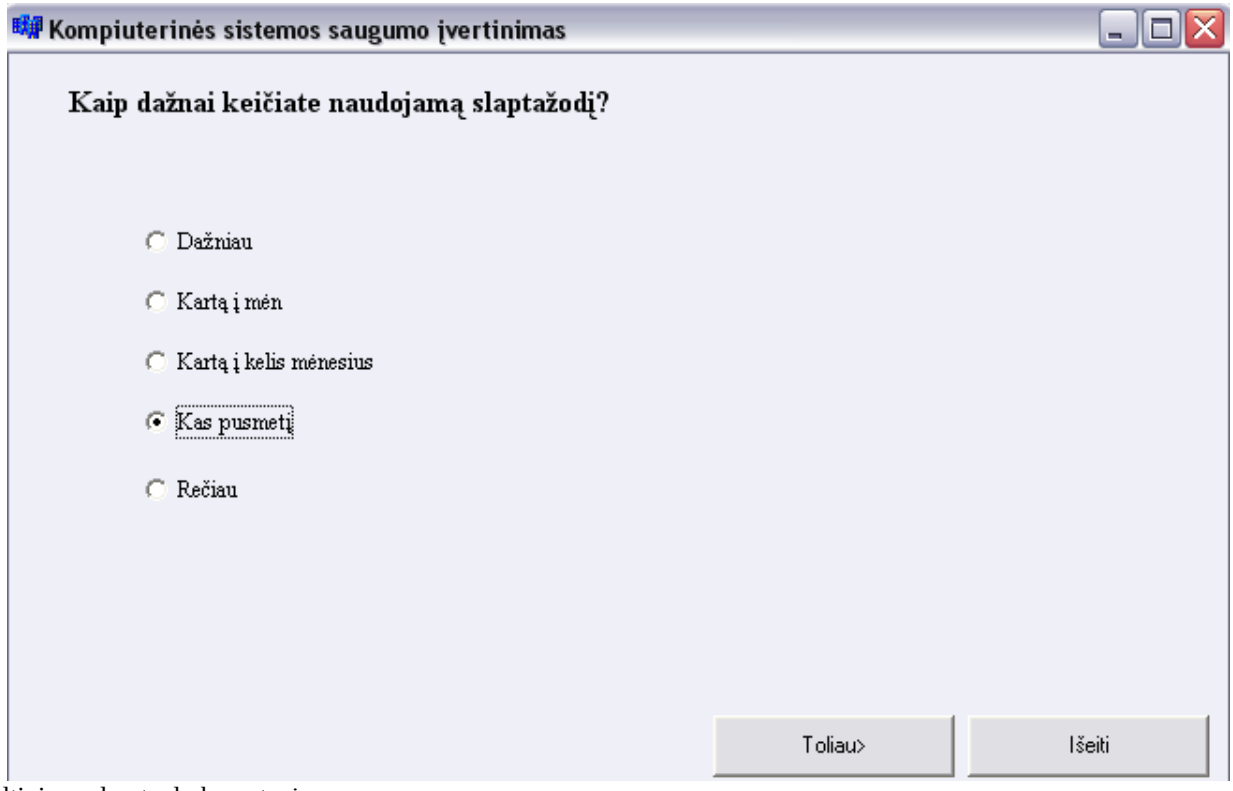
61 pav. Slaptažodžio patikimumo įvertinimas su specialia programa

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

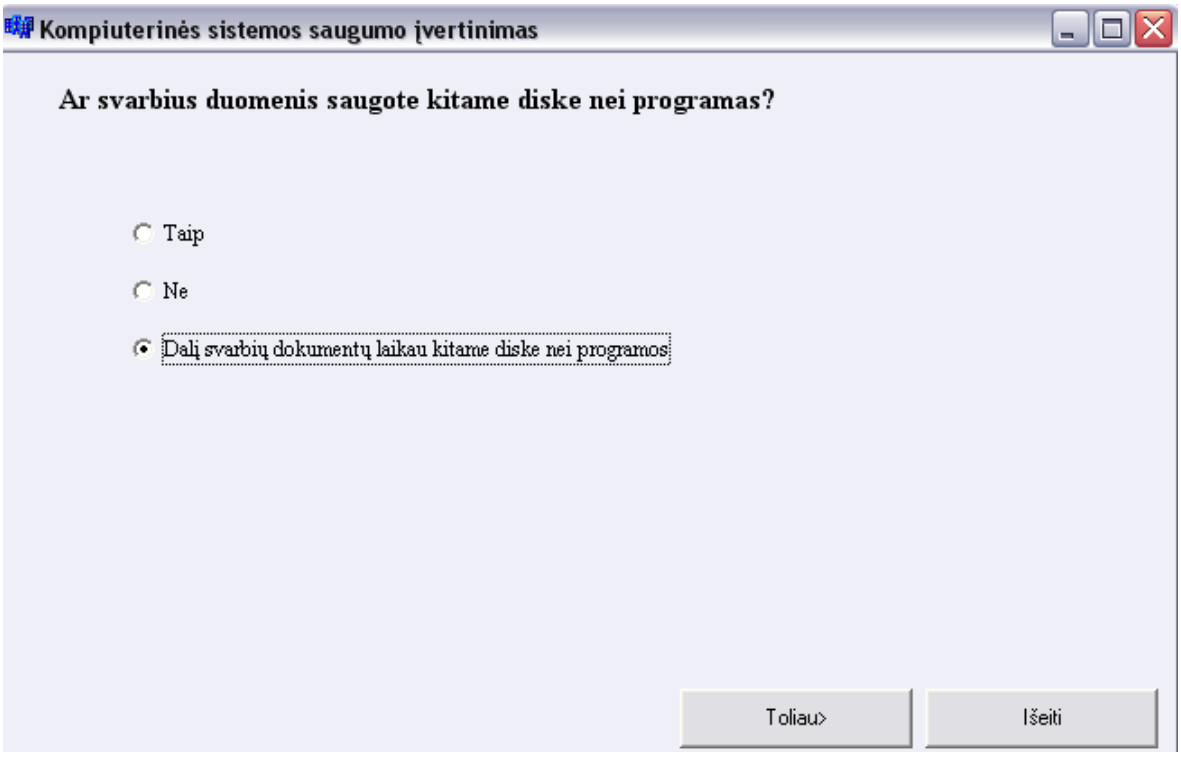
62 pav. Slaptažodžio keitimo įvertinimas



Šaltinis: sudaryta darbo autorės.

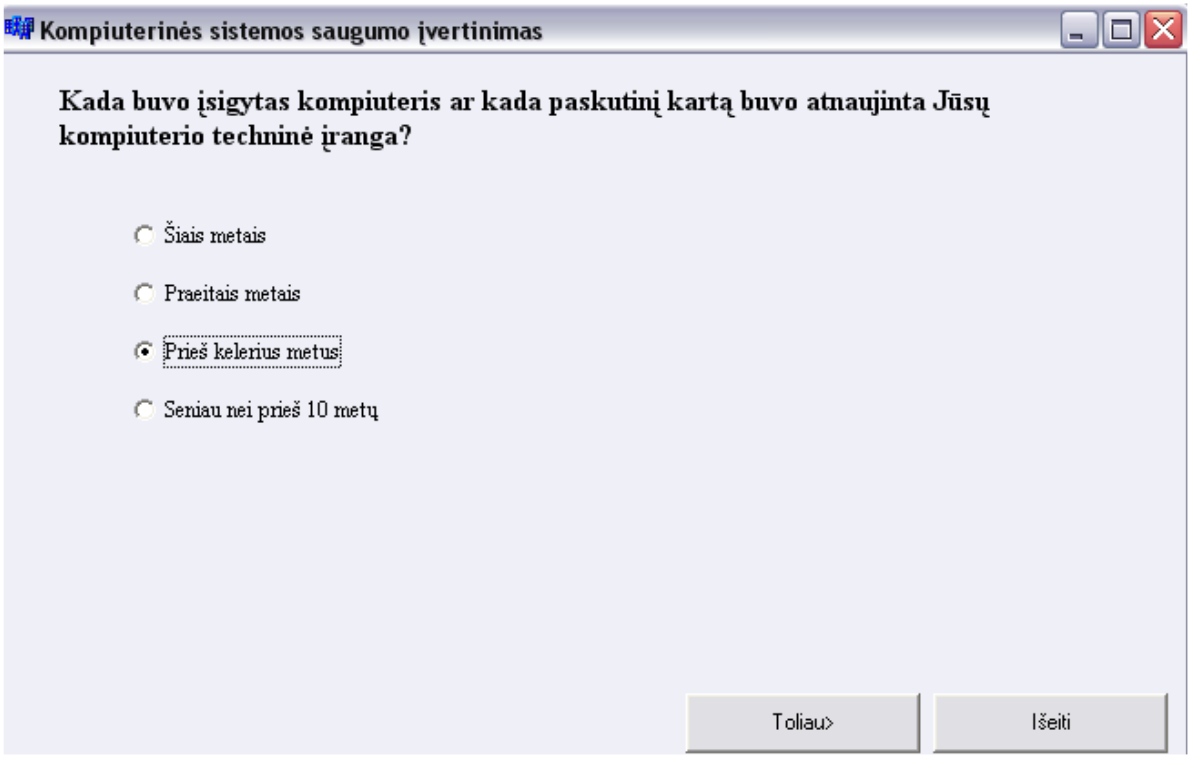
63 pav. Slaptažodžio keitimo dažnumas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

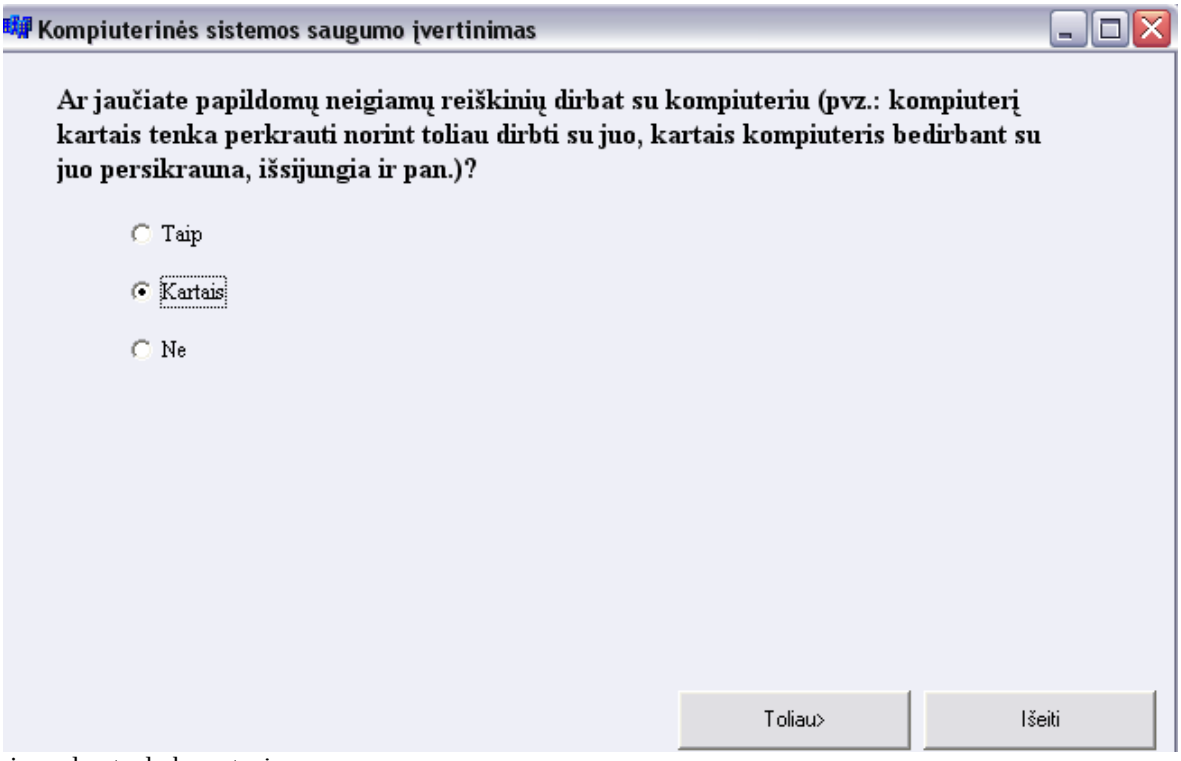
64 pav. Svarbių duomenų laikymo vietos kompiuteryje įvertinimas



Šaltinis: sudaryta darbo autorės.

65 pav. Kompiuterio įsigijimo laiko įvertinimas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



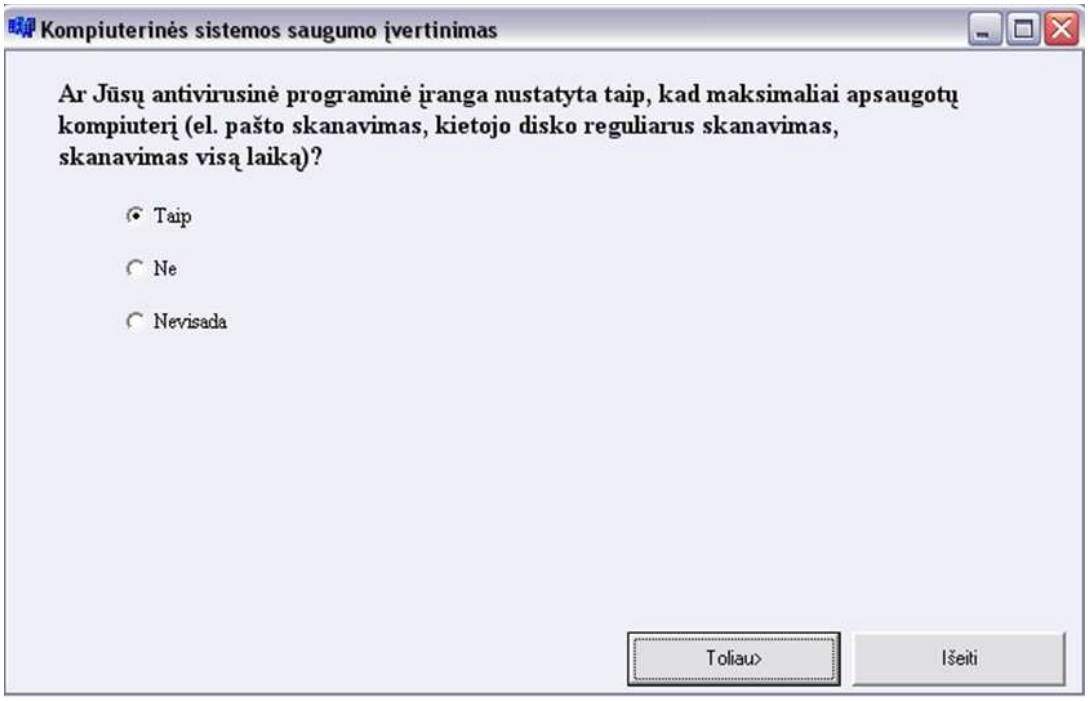
Šaltinis: sudaryta darbo autorės.

66 pav. Papildomų neigiamų reiškinių būvimo įvertinimas

Šaltinis: sudaryta darbo autorės.

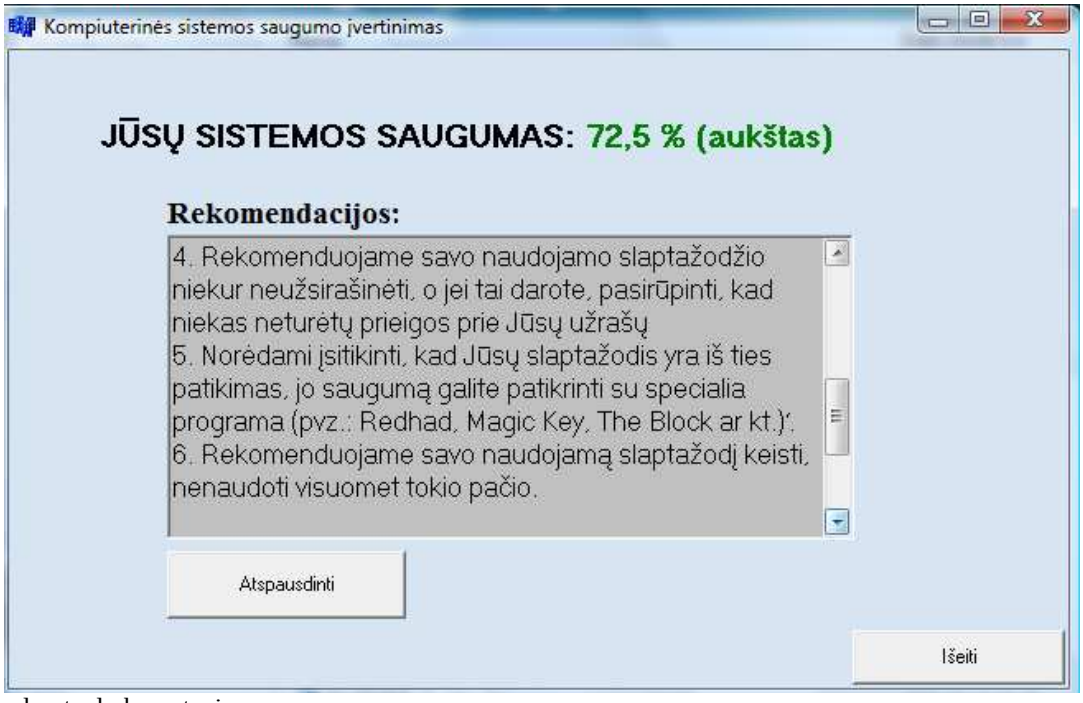
67 pav. Papildomų neigiamų reiškinių pasireiškimo dažnumas

Duomenų saugos įvertinimo programos lentelės bei pranešimai



Šaltinis: sudaryta darbo autorės.

68 pav. Papildomų neigiamų reiškinių būvimo įvertinimas



Šaltinis: sudaryta darbo autorės.

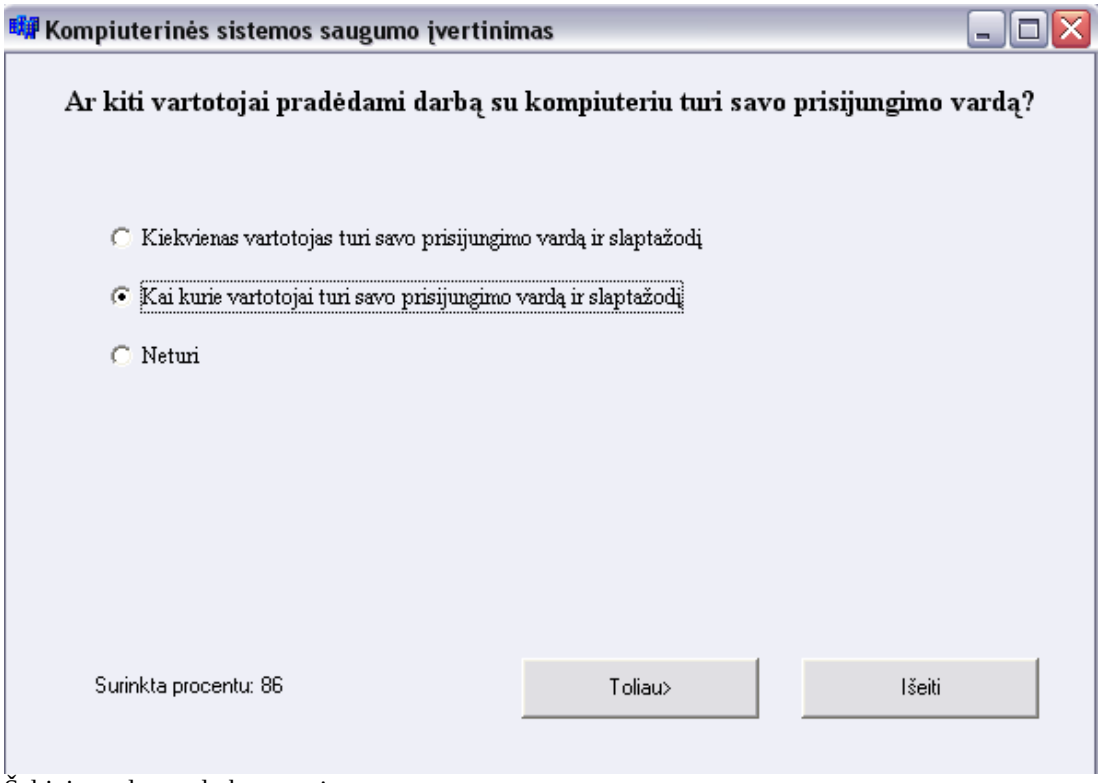
69 pav. Programos rezultatų išvedimas (plačiau 3.4 darbo skyrelyje)

2 PRIEDAS

Sistemos testavimas

Programos tekstas leidžiantis matyti tarpinius saugumo lygio įvertinimus:

Label5->Caption="Surinkra procentu: ";
Label5->Caption= Label5->Caption+minusuoti;



Šaltinis: sudaryta darbo autorės.

70 pav. Tarpinis duomenų saugumo lygio skaičiavimas

3 PRIEDAS

Konferencijoje pristatytas straipsnis

EKSPERTINĖ SISTEMA ĮVERTINANTI DUOMENŲ SAUGUMO LYGĮ

Rita Paulavičiūtė

Vilniaus Universiteto Kauno Humanitarinis Fakultetas, Muitinės g. 8, LT-44280 Kaunas

Santrauka. Duomenų laikomų kompiuteryje saugumu pradeda domėtis vis daugiau specialistų, nes nuolat kyla žmonių kompiuterizavimo lygis, didėja informacijos kiekiai bei dažnėja nesankcionuotas naudojimasis ja. Straipsnyje apžvelgiami metodai, kaip galima nustatyti duomenų saugumo lygį. Yra aprašytas procesas kaip buvo sukurta ekspertinė sistema, kuri įvertintų duomenų, laikomų kompiuteryje, saugumo lygį ir parinktų reikiamas duomenų apsaugos priemones saugumo lygio padidinimui. Straipsnyje pateikiami apibendrinti vartotojų atsiliepimai vertinant sistema, atsižvelgiant į juos programa buvo tobulinama.

Raktiniai žodžiai: duomenų saugumas, grėsmė, ekspertinė sistema.

1. Įvadas

Duomenų saugumu kompiuterinėse sistemose klausimais pradeda domėtis vis daugiau specialistų, tuo labiau, kad šios problemos sprendimui realų pagrindą suteikia ir vis tobulinama teisinė duomenų, ir informacijos apsaugos sistemos pusė. Vis didėjantys vertingos informacijos kiekiai bei kylantys žmonių kompiuterizavimo lygis, jų susidomėjimas kompiuterine informacija, sąlygoja vis dažniau pasitaikantį informacijos vogimą, nesankcionuotą bei neteisingą naudojimą. Pasirinkta sukurti ekspertinę sistemą, kuri įvertintų kompiuterio saugumą ir pasiūlytų reikiamas duomenų apsaugos priemones saugumo lygio padidinimui.

Duomenų apsaugos sistemų patikimumo įvertinimas - tai viena iš opiausių problemų su kuria susiduria IT specialistai. Duomenų apsaugos sistemų patikimumo įvertinimas yra galimas pagal daugelį metodų (kelis iš jų apžvelgsime šiame straipsnyje: tradicinis rizikos vertinimo metodas, saugumo klasės pagal „Oranžinę knygą“, ISO 15504 standartą, Shawn A. BUTLER siūlomas saugumo požymių įvertinimas pagal gaunamą naudą ir patiriamas išlaidas, RU security siūlomas metodas įvertinant verslo žlugimo tikimybę praradus duomenis, konfidencialumą bei duomenų vientisumą bei saugumo vertinimas pagal Informacijos saugumo sprendimus), bet nėra priimto vieningo duomenų apsaugos vertinimo metodo, tad susiduriama su problema, kad skirtingais metodais įvertinta ta pati kompiuterinė sistema yra vertinama skirtingai.

2. Saugumo nustatymo metodai

Norint nustatyti duomenų saugumo lygį, esantį kompiuteryje (kompiuterinėje sistemoje) galima naudotis įvairiais metodais, keletą iš jų apžvelgsime žemiau.

2.1. Tradicinis rizikos analizės metodas

Tradicinė rizikos analizė – tai netikėto įvykio atsitikimo ir jo pasekmių tikimybės matavimas. Pagal šį metodą rizika apytikriai yra prilyginama įvertinto kritinio įvykio tikimybės bei kainos susijusios su įvykiu sandaugai.

Vertinat saugumą remiantis šiuo metodu yra susiduriama su konkrečiam ir tiksliam įvertinimui kliudančiomis problemomis, nes „kaina“ gali turėti daug formų: pinigai (eurai, litai ar kita valiuta), prarastos gyvybės, gyvenimo paaukoti metai, prastovos valandų skaičius ir kt.

Tradicinis rizikos vertinimo metodas išsiskiria savo paprastumu, dėl to yra plačiai naudojamas, nes galimos reikšmės yra lengvai modeliuojamos. Tačiau skaičiuojant sistemos saugumą remiantis šiuo metodu susiduriama su neapibrėžtumu, nes kaina gali turėti daug formų. Tad remiantis šiuo metodu gaunami rezultatai yra gana subjektyvūs.

2.2. Kompiuterinio saugumo įvertinimas pagal ISO 15504 standartą

Pagal ISO 15504 standartą procesai gali būti suskirstyti į kategorijas: pirkėjo – pardavėjo, gamybos, antraeiliai, valdymo, organizavimo. Kiekvienam procesui ISO 15504 standartas apibrėžia jo pajėgumo lygį. Pajėgumas kiekvieno proceso yra nustatomas naudojant proceso atributus. Tarptautinis standartas išskiria devynis proceso atributus.

Kiekvienas proceso atributas yra detalizuojamas praktiškais rodikliais padedančiais įvertinti nagrinėjamą atributą. Kiekvienas proceso atributas yra vertinamas pagal keturių punktų vertinimo skalę.

ISO 15504 standartas - tai tarptautinis standartas, kuris kompiuterio saugumą vertina pagal jame vykstančius procesus, procesai savo ruoštu yra skirstomi į atributus, o atributai turi kelis įvertinimo lygmenis. Tokia kompiuterinio saugumo vertinimo metodika yra patikima ir ja remiantis organizacijos gali apibrėžti saugumo veiklas ir transformuoti jas į struktūras, koncentruotas į saugumą.

2.3. Saugumo klasės pagal „Oranžinę knygą“

„Oranžinėje knygoje“ apibrėžiami keturi saugumo lygiai (A, B, C, D, kur A klasė – tai aukščiausia saugumo klasė). Lygis D skirtas nesaugioms sistemoms, kurioms nekeliami jokie saugumo reikalavimai. Lygiai C ir B yra skirstomi į klases: C1, C2, B1, B2, B3, A1. Kiekvienai klasei taikomus reikalavimus galima suskirstyti į tokias grupes:

- reikalavimai kreipinių valdymo sistemai,
- reikalavimai registracijos ir apskaitos sistemai ir sistemos vientisumo,
- reikalavimai integralumo užtikrinimui.

Metodo trūkumas: klasės išskiriamos tiktai keturios, o dažniausiai aptinkamos kompiuterinės sistemos pasiskirsto tarp dviejų klasių (B ir C), nėra išvengiama subjektyvaus vertinimo, nes saugumo klasėje nėra apibrėžti visi galimi kompiuterinės sistemos komponentai.

Saugumo klasių klasifikacija pagal „Oranžinę knygą“ pasižymi aiškumu ir apibrėžtumu, bet vertinant kompiuterinę sistemą neišvengiama subjektyvumo, nes perėjimas tarp klasių nėra išsamiai apibrėžtas. Metodologija yra pritaikyta vertinti kompiuterines sistemas, o ne pavienius kompiuterius.

2.4. Rizikos įvertinimas pagal “Informacijos saugos sprendimus”

Rizikos vertinimo procesą būtų galima išskirti į keturis pagrindinius etapus:

- poveikio veiklai analizė,
- rizikos analizė, vertinimo bei saugumo valdymo priemonių pasirinkimas,
- rizikos lygio nustatymas, sprendimų radimas,
- rizikos valdymo proceso aprašymas.

Paskutinysis etapas apima visus tris prieš tai einančius etapus ir turi didžiausią išliekamąją vertę.

Rizikos įvertinimas remiantis „Informacijos saugos sprendimai“ siūloma metodika susideda iš šių etapų: poveikio veiklai ir rizikos analizė, saugumo vykdymo priemonių diegimo plano sudarymas bei rizikos valdymo proceso dokumentacija. Tyrimo šiuo metodu galutinis tikslas yra pateikti planą (kalendorinį tvarkaraštį), kuriuo remiantis atsispindėtų kas ir kada yra atsakingas už tam tikrų sprendimų atlikimą, priežiūrą, rizikos kiekio organizacijoje mažinimą.

2.5. RU Security siūlomas konfidencialumo rizikos vertinimo metodas

Riziką siūloma skirstyti i tris klases pagal RU security: konfidencialumo rizika, duomenų vientisumo rizika, prieinamumo arba verslo žlugimo rizika.

Konfidencialumo rizika nurodo neautorizuoto priėjimo prie informacinių išteklių (tokių kaip kliento informacija, slaptažodžiai, studentų pažymiai, tyrimų duomenys ir t.t.) įtaką. Duomenų vientisumo rizika apibūdina netikslių duomenų naudojimo riziką, netinkamiems verslo ar valdymo sprendimams priimti. Prieinamumo ar verslo žlugimo rizika apibūdina tikėtiną riziką sistemos klaidų ar nelaimės sukelto veiklos nutraukimo. Yra nagrinėjama įtaka tiek klientams, tiek atskiriems veiklos sektoriams.

Didžiausias keblumas šio metodo yra: kaip tiksliai nustatyti rizikos ir įtakos dydžius. Skaičiavimuose yra naudojami tik lingvistiniai terminiai „aukšta“, „vidutinė“, „žema“, tačiau kur nubrėžti ribas tarp šių dydžių nėra aišku. Tad yra sunku įvertinti duomenų svarbą arba galimos žalos dydį remiantis šiuo metodu.

RU security metodo pagalba galima lengvai modeliuoti galimas reikšmes trijose kategorijose (konfidencialumo, duomenų vientisumo, verslo žlugimo rizikos vertinime), tačiau pastebėtina, kad gauti rezultatai yra daugiau tikėtini nei realūs (tikslūs), nes ribos tarp reikšmių „aukšta“, „vidutinė“, „žema“ nėra apibrėžtos, o yra nustatomos subjektyviai.

Konferencijoje pristatytas straipsnis

2.6. Shawn A. BUTLER siūlomas saugumo požymių įvertinimo išlaidų ir gaunamos naudos metodas

Naudojantis šiuo metodu IT specialistas apskaičiuoja, kokia yra tikimybė patirti grėsmę lygią nuo 2-3 kartų per valandą iki 2-3 kartų per metus. Po pirminio grėsmių tikimybių sudėliojimo IT specialistas įvertina grėsmes skalėje nuo1 iki 100. Atributas keliantis daugiausiai nerimo gauna įvertinimą lygu 100 balų. Taip yra įvertinami visi atributai, galiausiai suskaičiuojamos jų vertės skalėje nuo 0 iki 1.

Kiekvienai atakai yra apskaičiuojama kiekvieno IT specialisto subjektyviai priskirtai vertė bei tikimybė. Grėsmės tikimybės reikšmė yra skirtinga keičiantis rizikos grėsmės lygiui. Kiekviena pasirinkta atakos grėsmė apskaičiuojama atskirai įvertinant jos pasirodymo galimybę (retai, kartais ir dažnai).

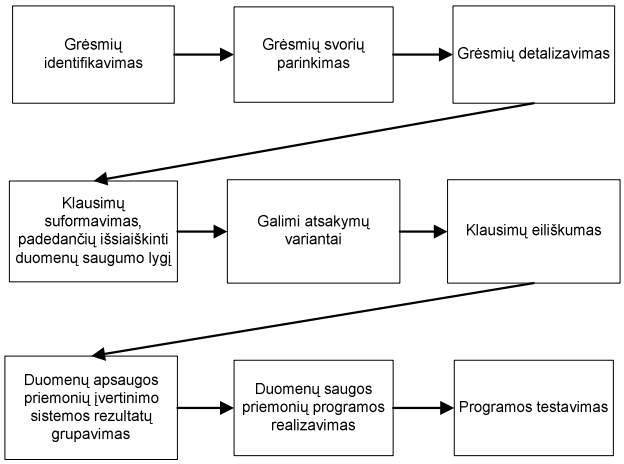
Išlaidų bei gaunamos naudos metodo rezultatais galima pasikliauti tik tuo atveju jeigu kompiuterinę sistemą vertina kvalifikuotas IT specialistas, nes suteikiama teisė pačiam specialistui įvertinti grėsmių svarbą. Jei specialistas nėra tikras savo srities žinovas - jo priimtos prielaidos vėliau paaiškės buvusios neteisingos ir organizacija bus investavusi į mažiau svarbias vietas savo informacinio saugumo užtikrinimui.

3. Rezultatai

Išnagrinėjus įvairius duomenų saugumo priemonių vertinimo metodus nutarta kurti ekspertinę sistemą, kuri duomenų saugumą vertintu šiais aspektais:

- slaptažodžio buvimas, jo saugumas,
- antivirusinės programos buvimas,
- operacinės sistemos legalumas,
- naudojamų programų legalumas,
- šiukšlių patekimo į kompiuterį rizikos įvertinimas,
- ugniasienės buvimas (jei kompiuteris turi išeigą į internetą),
- kompiuterio laikomo vietos saugumas,
- vartotojų (-o) besinaudojančių (-io) kompiuteriu patikimumas,
- papildomų laikmenų prijungimo prie kompiuterio dažnumas,
- duomenų kopijų darymas bei jų laikymo vietos patikimumas,
- itin svarbių duomenų turėjimas,
- diegimas į kompiuterį abejotinos vertės programų.

Duomenų saugos priemonių saugumo lygio nustatymo eiga yra pavaizduota 1 paveikslėlyje. Grėsmė - tai pavojus tykantis duomenų esančių kompiuteryje. Sekantis ne ką mažiau svarbus žingsnis – yra svorių parinkimas nustatytoms grėsmėm. Svoris – tai koeficientas, nustatantis grėsmės galimą padaryti žalą duomenų saugumui.



1 pav. Duomenų apsaugos priemonių nustatymo procesas

Žinant duomenų saugumui kylančias grėsmes bei jų galimą padaryti žalą buvo atsižvelgta, kad ta pati grėsmė skirtingose situacijose gali būti skirtingai žalinga. Niekas nepaneigs, kad virusų patekimas yra grėsmingas procesas kompiuteryje saugomų duomenų saugumui, tačiau vertinant duomenų apsaugos lygį skirtingai būtų vertinamas virusas,

kuris sutrikdė įprastą kompiuterio vartotojo dienotvarkę ar kurio būvimas kompiuteryje nepadarė jokios žalos ir buvo laiku pašalintas. Vertinant virusų būvimo kompiuteryje žalą yra atsižvelgiama ir į tai ar virusų padaryta neigiama įtaka yra juntama kiekvieną savaitę ir ji buvo juntama vieną kart per pastarąjį pusmetį.

Turint apibrėžtas, detalizuotas grėsmes bei žinant jų svorius buvo suformuoti klausimai, kurie padėtų nustatyti duomenų saugos lygį. Sugalvojus klausimus bei galimus atsakymus buvo sudarytas klausimų pateikimo eiliškumas. Prieš realizuojant programą reikėjo apsispręsti, kaip pateikti duomenų saugumo įvertinimo rezultatą klientui, kad gauti rezultatai būtų aiškūs ir suprantami. Nuspręsta rezultatus pateikti tiek vertinant 100 % skalėje, tiek raštu pateikiant patarimus vartotojui.

Žinant, kokius klausimus ir kada pateikti vartotojui, kaip vertinti galimus atsakymus ir kaip pateikti gautus rezultatus buvo realizuota duomenų saugumo priemones įvertinanti programa. Duomenų saugumo lygis yra vertinamas šimto balų sistemoje. Programa ne tik pateikia duomenų saugumo lygio įvertinimą, bet ir pataria, kokių veiksmų reikėtų imtis norint padidinti duomenų saugumo lygį.

Sukurta ekspertinė sistema atsižvelgia ne tik į kompiuteryje įdiegtas programas, jų legalumą, bet ir į vartotojo atliekamus veiksmus, nes net turint visą reikiamą programinę įrangą, bet netinkamai su ja elgiantis yra sumažinamas kompiuteryje esančių duomenų saugumo lygis.

Sukūrus programą buvo nuspręsta įvertinti programos veikimą. Programa buvo duota testuoti žmonėms, kurie vertino savo turimo kompiuterio duomenų daugumo lygį.Buvo apklausti 103 respondentai. Norint, kad programa būtų išsamiai įvertinta, programą vertino skirtingo amžiaus žmonės (apklaustųjų žmonių amžius nuo 17 iki 66 metų), skirtingų socialinių grupių žmonės (bedarbiai, moksleiviai, studentai, darbdaviai, samdomi darbuotojai, pensininkai). 47 apklaustieji neturėjo jokių komentarų, pastabų programos veikimui (tai sudaro 45,6% iš visų apklaustųjų). Likusių (54,4% iš visų apklaustųjų arba 56 žmonių) respondentų išsakytos apibendrintos pastabos pateiktos 1 lentelėje.

1 lentelė. Vartotojų išsakytos pastabos bei padaryti pataisymai

Nr.	Pastabos
1	Reikia padaryti, kad vartotojo sąsaja būtų draugiškesnė.
2	Reikia įvertinti kokia antivirusine programa yra naudojamasi (pagal pavadinimą, pagal versijos naujumą, pagal nustatytus parametrus joje).
3	Reikia įvertinti kompiuterio būklę.
4	Reikia įvertinti slaptažodžių saugumą, išsiaiškinant ar jis yra įvertintas pagal specialias programas bei įvertinti slaptažodžio keitimo dažnumą.
5	Reikia įvertinti papildomas sąlygas dirbant su kompiuteriu (pvz. naudojamas papildomas saugumą užtikrinančias programas ir kt.)
6	Reikia keisti kelių klausimų formulavimą, nes nėra aišku ko klausiama.

Atsižvelgiant į vartotojų pastabas buvo pakeistas kelių klausimų formulavimas, įtraukti papildomi klausimai padedantys įvertinti duomenų saugumo lygį kompiuteryje. Siekiant draugiškesnės vartotojo sąsajos programoje padaryti šie pakeitimai: pateikiant rekomendacijas įvesta numeracija, padaryta galimybė ne tik peržiūrėti, bet ir atsispausdinti jas, vartotojas prieš pradėdamas atsakinėti į klausimus yra informuojamas kaip bus pateikiami klausimai bei kaip reikės žymėti tinkamus atsakymus.

4. Išvados

Siekiant pagrindinio tikslo, sukurti ekspertinę sistemą, kuri įvertintų duomenų laikomų kompiuteryje apsaugos priemonių saugumo lygį ir parinktų reikiamas duomenų apsaugos priemones saugumo lygio padidinimui, straipsnyje yra išanalizuoti duomenų saugumo priemonių nustatymo metodai, sukurta ekspertinė sistema bei surinkta vartotojų nuomonė apie ją.

Sukurtos sistemos pranašumas - tai galimybė neišeinant iš namų ir be papildomų lėšų įvertinti duomenų saugumo lygį, esantį kompiuteryje bei išsiaiškinti, kokių konkrečių žingsnių reikia imtis didinant duomenų saugumo patikimumo lygį. Sukurta sistema palengvina kompiuterio vartotojų dedamas pastangas išsiaiškinti duomenų saugumo lygį esantį kompiuteryje bei taupo laiką, skiriamą saugumo lygio pagerinimui.

Atsižvelgiant į programos vartotojų poreikius bei pastabas ateityje programos veikimo spektras gali būti plečiamas ir pritaikytas ne tik pavienio kompiuterio vertinimui, bet ir kompiuterinės sistemos saugumo vertinimui.

Konferencijoje pristatytas straipsnis

Literatūra

[1] MEHROTRA, S.; BUTTS, C, KALASHNIKOV, D.; VENKATASUBRAMANIAN, N. (2004) Project Rescue: Challenges in Responding to the Unexpected [interaktyvus]. [žiūrėta 2007 m. rugsėjo 02 d.]**.** Prieiga per internetą http://www.ics.uci.edu/~dvk/pub/SPIE04dvk.pdf .

[2] DUNCAN, George T.; KELLER-MCNULTY, Salvie A.; ir STOKES, S. Lynne. (2004) Data Utility through the R-U Confidentiality Map [interaktyvus]. [žiūrėta 2008 m. balandžio 15 d.]**.** Prieiga per internetą http://www.niss.org/technicalreports/tr121.pdf.

[3] BUTLER, Shawn A. (2002) Security Attribute Evaluation Method: A Cost-Benefit Approach [interaktyvus]. [žiūrėta 2008 m. vasario 26 d.]**.** Prieiga per internetą <http://portal.acm.org/citation.cfm?id=581370 >.

[4] Softweare Quality. (2008) [interaktyvus]. [žiūrėta 2008 m. birželio 15 d.]. Prieiga per internetą <http://software-quality.blogspot.com/2006/10/risk-based-selection-for-agile.html>.

[5] Electronic Orange Book. (2008) [interaktyvus]. [žiūrėta 2008 m. balandžio 17 d]. Prieiga per internetą <http://www.fda.gov/cder/ob/>.

[6] Rutgers secure. Risk Assessment. (2008) [interaktyvus]. [žiūrėta 2008 m. balandžio 19 d.]. Prieiga per internetą <http://rusecure.rutgers.edu/sec_plan/risk.php>.

The Expertise System for Information Security

There are overlooked various of the method how to protect security level in this article. The main goal of the article is creation the expertise system for evaluation data security, which are in computer and recommend how to expand security level and to test the system. The main advantages of new system are: user in very quick way can to know how reliable data in the computer are and he also could know the ways how to make data security level more reliable.