

(Author Name, Surname)

(Name of the Thesis)

(Header Page No. 1)

(Head of Department Name, Surname, Signature)

(Name of the Thesis)

(Header Page No. 2)

(Author Name, Surname)

(Academic Supervisor Name, Surname, Signature)

(Consultant Name, Surname, Signature)

(Head of Department Name, Surname, Signature)

(Author Name, Surname)

(Name of the Master Thesis)

(Order No and Date for confirming the existence of the Project)

(Main Tasks of the Master Thesis)

(Author Name, Surname, Signature)

(Academic Supervisor Name, Surname, Signature)

Vilniaus Gedimino technikos universitetas

ISBN ISSN

Egz. sk.

Data-

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

Pavadinimas **(Name of the Thesis)**

Autorius (Author Name, Surname)

Vadovas (Supervisor Name, Surname)

Kalba

X

lietuvių

užsienio

Anotacija

Nuo tada, kai įvairios vyriausybinės ir nevyriausybinės įstaigos ar tarptautinės organizacijos pradeda rūpintis savo informacijos ar kitų valdomų vertybių saugumu, jos bando sukurti ar nusipirkti informacijos saugumo sistemų sprendimus, kurios padidina biudžeto išlaidas, o dalis šių sistemų néra pritaikytos ir tinkamos užtikrinti įstaigos informacijos saugumą, nes néra lankscios, sunku išplėsti jų funkcionalumą, nesuteikia galimybės vizualiai atsižvelgti į esamą dabartinę padėtį bei kylančias naujas grėsmes.

Šiame magistro darbe bus įvertintos galimybės parengti grėsmių vizualizacija paremtą informacijos saugos valdymo informacinės sistemos prototipą, kuris, atsižvelgiant į šiu dienų informacijos saugos pagrindinius principus ir reikalavimus, būtų lankstus, lengvai praplečiamas, leistų įtraukti kasdieninį įstaigos ar organizacijos vertybių valdymą, suteiktų galimybę už saugumo priežiūrą atsakingiems specialistams įvertinti įstaigai ar organizacijai kylančias grėsmes bei rizikas šioms grėsmėms atsirasti, pritaikant 3D vizualizacijos technologiją. Prieš pradedant kurti sistemos prototipą bus atlikta panašaus pobūdžio sistemų analizė ir nagrinėjami šių sistemų veikimo principai informacijos saugos užtikrinimo klausimu. Vėliau seks projektavimo darbai, vizualizacijos technologijos pasirinkimas, sistemos prototipo kūrimas, bandymai, rezultatų apibendrinimas ir išvados.

Darbą sudaro 6 dalys: įvadas, susijusios literatūros analizė, grėsmių vizualizavimo metodas, grėsmių vizualizavimo metodo realizacija, bandymų atlikimas, išvados ir siūlymai, literatūros sąrašas.

Darbo apimtis – 94 p. teksto be piedų, 37 iliustr., 14 lent., 40 bibliografinių šaltinių.

Atskirai pridedami darbo piedai.

Prasminiai žodžiai: saugumo grėsmės, informacijos sauga, informacinė sistema, informacijos saugos valdymas, 3D vizualizacija.

Vilnius Gediminas Technical University

ISBN ISSN

Copies No.

Date-.....

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

Title **(Name of the Thesis)**

Author (Author Name, Surname)

Academic supervisor (Supervisor Name, Surname)

Thesis language



Lithuanian



Foreign(English)

Annotation

Since various governmental and non-governmental institutions and organizations are concerned about their information and other assets, they tend buy or develop various information security systems. It increases costs drastically and yet many of the systems are not appropriate to ensure the organization's information security. The solutions are not flexible and functionally scalable, does not take into account the possibilities to visualize current state and to detect emerging threats.

This master thesis will evaluate the feasibility of developing the threat visualization based information security management system prototype that takes into consideration the latest information security principles and requirements, is flexible and extendable. The prototype would function as a part of organization's assets management process and would provide an opportunity for security professionals to assess the organization's security threats with a help of the 3D visualization technology and mitigate risks for these threats to arise.

Before the system prototype development commences, similar existing systems will be analyzed considering the operational principles of these systems from information security perspective. Afterwards, system design activities, a selection of the visualization technology, prototyping, testing and defect fixing will be carried out. Finally, the prototype will be evaluated to summarize results and draw conclusions.

The paper comprises of 6 sections: introduction, related literature analysis, description of the proposed threat vizualization method, implementation of the proposed method, test realization, conclusions and suggestions section and references.

The Thesis contains of 94 text pages (without appendixes), 37 pictures, 14 tables, 40 bibliographical entries.

Appendices included.

Keywords: security threats, information security, information system, information security management, 3D visualization.

(Head of Department Name, Surname, Signature)

(Declaration of the Authorship in the Final Degree Project)

(Order No and Date for confirming the existence of the Project)

(Academic Supervisor Name, Surname)

(Author Name, Surname, Signature)

(From 2018-2019 It's required to provide the Page
to allow or forbid the use of the Project)

(Automatically all previous Projects are considered as Not Available
without Authors consent)

Turinys

1.	Įvadas.....	15
1.1.	Tyrimo objektas.....	16
1.2.	Darbo tikslas ir uždaviniai.....	16
1.3.	Temos naujumas	17
1.4.	Temos aktualumas	17
1.5.	Tyrimo metodika	18
1.6.	Mokslinė darbo vertė	18
1.7.	Darbo rezultatai	18
1.8.	Darbo struktūra.....	20
1.9.	Darbo aprobacija	20
2.	Susijusios literatūros analizė	21
2.1.	Informacijos saugumo valdymo problema	21
2.2.	Vizualizacijos saugos sistemų sprendimai	23
2.2.1.	Saugumo standartų žymėjimo vizualizacija	23
2.2.2.	Saugumo analizė ir vizualizacija su „LYNXeon™“	25
2.2.3.	Saugumo analizė ir vizualizavimas su „CiscoWorks“ SIMS	26
2.2.4.	Atakų vizualizavimas su CySeMoL	26
2.3.	Vizualizacijos technologijos.....	28
2.3.1.	„Adobe Flash“	28
2.3.2.	HTML 5 „Canvas“.....	29
2.3.3.	SVG	30
2.3.4.	CSS	30
2.3.5.	JavaFX	30
2.3.6.	WebGL	31
2.4.	Vizualizacijos technologijos pasirinkimas	32
2.5.	Antro skyriaus apibendrinimas ir pagrindiniai rezultatai	33
2.6.	Antro skyriaus išvados	34
3.	Grėsmių vizualizavimo metodas	36
3.1.	Grėsmių vizualizavimo metodo schema.....	38
3.2.	Grėsmių vizualizavimo metodo tekstinis aprašas.....	39
3.3.	Grėsmių vizualizavimo eksplikacijos schema	41
3.4.	Grėsmių vizualizavimo eksplikacijos tekstinis aprašas.....	42
3.5.	Trečio skyriaus apibendrinimas ir pagrindiniai rezultatai	43
3.6.	Trečio skyriaus išvados	43
4.	Grėsmių vizualizavimo metodo realizacija, bandymų atlikimas.....	45
4.1.	Grėsmių vizualizavimo prototipo reikalavimų specifikacija.....	45
4.1.1.	Vartotojo sąsajos reikalavimai	45
4.1.2.	Funkciniai reikalavimai	65
4.1.3.	Nefunkciniai reikalavimai	67
4.2.	Grėsmių vizualizavimo prototipo bandymai	72
4.2.1.	GVSRU-1 užduoties bandymas.....	72
4.2.2.	GVSRU-2 užduoties bandymas.....	73
4.2.3.	GVSRU-3 užduoties bandymas.....	73
4.2.4.	GVSRU-4 užduoties bandymas.....	74
4.2.5.	GVSRU-5 užduoties bandymas	76
4.2.6.	GVSRU-6 užduoties bandymas.....	77
4.2.7.	GVSRU-7 užduoties bandymas	78
4.2.8.	GVSRU-8 užduoties bandymas	80
4.2.9.	GVSRU-9 užduoties bandymas	82

4.2.10. GVSRU-10 užduoties bandymas.....	83
4.2.11. GVSRU-11 užduoties bandymas.....	84
4.3. Ketvirto skyriaus apibendrinimas ir pagrindiniai rezultatai	86
4.3.1. Grėsmių vizualizavimo prototipo privalumai.....	86
4.3.2. Grėsmių vizualizavimo prototipo trūkumai.....	87
4.4. Ketvirto skyriaus išvados	87
5. Išvados	89
6. Literatūros sąrašas	91
Priedai.....	96
A Priedas. Grafinė vartotojo sąsaja	97
B Priedas. Langu maketai ir piktogramos	98
C Priedas. Užduočių formulavimo būdo reikalavimų dalis.....	102

Paveikslų sąrašas

1 pav. Standartinė žymėjimo vizualizacija naudojant grafių struktūrą [13]	23
2 pav. Standartinė žymėjimo vizualizacija naudojant „Chord“ diagramą [13]	24
3 pav. Kenksmingo kodo paplitimo tinklo tyrimas [15]	25
4 pav. Tinklo vizualizacija [15]	25
5 pav. Tinklo vizualizacija [16]	26
6 pav. CySeMoL modelio dalis	27
7 pav. WebGL pažeidžiamumas ankstyvojoje išleidimo stadijoje [33]	32
8 pav. Istaigos vertybės rizikos laipsniai	38
9 pav. Grėsmių vizualizavimo metodo schema	39
10 pav. Grėsmių vizualizacijos metodo eksplikacijos schema	42
11 pav. GVSRU-9 užduoties sekų diagrama	60
12 pav. GVSRU-10 užduoties sekų diagrama	63
13 pav. GVSRU-11 užduoties sekų diagramos dalis	64
14 pav. Komponentų pasiskirstymas kompiuterių tinkle schema	67
15 pav. „Istaigos“ meniu skyriaus „Struktūrių padalinį sąrašas“ poskyris	74
16 pav. „Vertybės“ meniu skyriaus „Vertybės“ poskyris	75
17 pav. „Inventorius“ meniu skyriaus „Inventorius“ poskyris	76
18 pav. „Rizikos valdymas“ meniu skyriaus „Priskyrimas“ poskyris	78
19 pav. „Rizikos valdymas“ meniu skyriaus „Nustatymai“ poskyris	79
20 pav. „Rizikos valdymas“ meniu skyriaus „Rizikos valdymas“ poskyrio ataskaitos rizikos vertinimas	81
21 pav. „Rizikos valdymas“ meniu skyriaus „Rizikos valdymas“ poskyrio ataskaitos rizikos tvarkymas	81
22 pav. Rizikos valdymo ataskaitos spausdinimas PDF formatu	82
23 pav. „Saugos vizualizacija“ meniu skyriaus „Objektų struktūra“ poskyris	83
24 pav. „Saugos vizualizacija“ meniu skyriaus „Rizikos vizualizavimas“ poskyris	84
25 pav. „Rizikos valdymas“ meniu skyriaus „Rizikos valdymas“ poskyrio ataskaitų rizikos lygio palyginimo lentelė	85
26 pav. „Rizikos valdymas“ meniu skyriaus „Rizikos valdymas“ poskyrio ataskaitų rizikos lygio palyginimo lentelė su detaliu vertybų ir jų rizikos laipsnių sąrašu	85
27 pav. GVSRU-1 užduoties sekų diagrama	102
28 pav. GVSRU-2 užduoties sekų diagrama	105
29 pav. GVSRU-3 užduoties sekų diagramos dalis	107
30 pav. GVSRU-3, GVSRU-4, GVSRU-5 užduočių sekų diagramos dalis	108
31 pav. GVSRU-5 užduoties sekų diagramos dalis	112
32 pav. GVSRU-6 užduoties sekų diagramos dalis	113
33 pav. GVSRU-6 užduoties sekų diagramos dalis	114
34 pav. GVSRU-6 užduoties sekų diagramos dalis	115
35 pav. GVSRU-7 užduoties sekų diagrama	120
36 pav. GVSRU-8 užduoties sekų diagramos dalis	123
37 pav. GVSRU-8 užduoties sekų diagramos dalis	124

Lentelių sąrašas

1	lentelė. Vizualizacijos technologijų kriterijų lyginamoji lentelė.....	33
2	lentelė. GVSRU-1 užduoties aprašas	46
3	lentelė. GVSRU-2 užduoties aprašas	46
4	lentelė. GVSRU-3 užduoties aprašas	47
5	lentelė. GVSRU-4 užduoties aprašas	48
6	lentelė. GVSRU-5 užduoties aprašas	49
7	lentelė. GVSRU-6 užduoties aprašas	50
8	lentelė. GVSRU-7 užduoties aprašas	52
9	lentelė. GVSRU-8 užduoties aprašas	53
10	lentelė. GVSRU-9 užduoties aprašas	53
11	lentelė. GVSRU-10 užduoties aprašas	54
12	lentelė. GVSRU-11 užduoties aprašas	54
13	lentelė. GVSRU užduočių formavimo kalba.....	55
14	lentelė. Piktogramų sąrašas	101

Santrumpų sąrašas

2D – angl. *Two-dimensional* – geometrinis 2 parametrų modelis

3D – angl. *Three-dimensional* – geometrinis 3 parametrų modelis

API – angl. *Application Programming Interface* – taikomosios programos sąsaja

CySeMoL – kibernetinio saugumo modeliavimo kalba

CSS – angl. *Cascading Style Sheet* – kalba, kuri nusako kitomis struktūrinėmis kalbomis aprašytų dokumentų vaizdavimą

DAC – angl. *Discretionary Access control* – diskretinė prieigos kontrolė

DOM – angl. *Document Object Model* – dokumento objekto modelis

EAAT – angl. *Enterprise Architecture Analysis Tool* – verslo architektūros analizės įrankis

ECMA – angl. *European Computer Manufacturers Association* – Europos kompiuterių gamintojų asociacija

HTML – angl. *HyperText Markup Language* – kompiuterinė žymėjimo kalba, naudojama pateikti turinį interne

HTTP – angl. *Hypertext Transfer Protocol* – pagrindinis metodas pasiekti informaciją interne

IBEB – angl. *Image-Based Edge Bundles* – nuotraukos pagrindu briaunos rinkiniai

IDS – angl. *Intrusion Detection System* – įsilaužimų aptikimo sistema

IPS – angl. *Intrusion Prevention System* – įsilaužimų sustabdymo sistema

ISACA – angl. *Information Systems Audit and Control Association* – tarptautinė organizacija, vienijanti informacinių technologijų specialistus, kurie kuria informacinių technologijų vadybos ir audito standartus, atlieka tyrimus šioje srityje, skleidžia savo patirtį ir skatina efektyvų informacijos, sistemų ir technologijų valdymą

IT – angl. *Information technology* – informacinės technologijos

JRE – angl. *Java Runtime Environment* – „Java“ programavimo kalbos paleidimo aplinka

MAC – angl. *Mandatory access control* – mandatinė prieigos kontrolė

MTL – angl. *Material library* – medžiagų rinkinio formatas

MVC – angl. *Model-View-Controller* – programinės įrangos architektūros modelis, kuris kompiuteryje įgyvendina vartotojo sąsają

NIST – angl. *National Institute of Standards and Technology* – Nacionalinio standartų ir technologijų institutas

OBJ – angl. *Object* – objekto formos formatas

OCL – angl. *Object Constraint Language* – deklaratyvi ribojimų kalba

PCI DSS – angl. *Payment Card Industry Data Security Standard* – mokėjimo kortelių industrijos duomenų saugumo standartas

PDF – angl. *Portable Document Format* – dvimačio elektroninio dokumento atvaizdavimo formatas

PHP – angl. *Hypertext Preprocessor* – dinaminė interpretuojama programavimo kalba

PNG – angl. *Portable Network Graphics* – bitų masyvo formatas

RBAC – angl. *Role-based access control* – vaidmenimis grindžiama prieigos kontrolė

SCADA – angl. *Supervisory Control and Data Acquisition* – centralizuota sistema ar sistemų rinkinys, kuris renka duomenis, atlieka visos sistemos stebėjimą ir vykdo jos kontrolę

SEO – angl. *Search Engine Optimization* – optimizavimas paieškos sistemoms

SIMS – angl. *Security Information Management Solution* – saugumo informacijos valdymo sprendimas

SVG – angl. *Scalable Vector Graphics* – XML pagrindu paremtas vektorinių nuotraukų formatas

SWF – angl. *Small Web File* – „Adobe Flash“ rinkmenos formatas

TCP/IP – angl. *Transmission Control Protocol/Internet Protocol* – standartinis duomenų perdavimo protokolų rinkinys, kurio pagrindu veikia internetas bei daugelis privačių komercinių tinklų

UML – angl. *Unified Modeling Language* – vieninga modeliavimo kalba

WebGL – angl. *Web Graphics Library* – „JavaScript“ API interaktyvaus 3D ir 2D grafikos atvaizdavimui interneto naršyklėje nereikalaujant papildomų įskiepių

XLS – angl. *Microsoft Excel spreadsheet* – dinaminė elektroninė lentelė

XML – angl. *Extensible Markup Language* – žymėjimo kalba, aprašyta XML 1.0 specifikacijoje

1. Įvadas

Paskutiniai dešimtmečiai informacinių technologijų apimtis išaugo dešimtadalį karto, tuo pačiu išaugo ir informacijos saugumo poreikis, kuris kelia rūpesčių visų tipų organizacijoms – tiek privataus verslo, tiek vyriausybinio sektoriaus. Įmonės bando keistis išlikdamos konkurencingos besikeičiančioje globalioje rinkoje, o vyriausybinės įstaigos siekia teikti geresnes paslaugas savo piliečiams [1].

Naujos sistemos ir protokolai buvo kuriami ir pritaikomi informacijos saugumui užtikrinti ir užkirsti kelią kompiuterinių tinklų įsibrovėliams. Šie pasiekimai bei visa informacinių technologijų raida priklauso nuo žmonių, kurie vis dar yra svarbūs kompiuterių ir informacijos saugos procese. Administratoriai turi kantriai stebėti informacijos mainus, rinkti duomenis kompiuterių tinkle ir priimti atitinkamus veiksmus, kad būtų užtikrintas informacijos saugumas organizacijoje. Jie turi bendradarbiauti ir koordinuoti veiksmus su savo kolegomis. Žmonės šiandien yra informacijos saugumo centre, taip pat kaip ir prieš tuos kelis paskutiniuosius dešimtmečius. Nors tobulėjančios informacinės technologijos ir dauguma procesų yra automatizuojami, tačiau analitiniai sugebėjimai ir žmonių išradingumas yra vieni iš svarbiausių pritaikomų pavyzdžių informacijos saugumo procese. Būtent dėl to visas informacijos saugos analitinis darbas neturėtų arba iš dalies galėtų būti automatizuotas naudojant SCADA sistemas.

Žmonės linkę suteikti saugumo terminui daug prasmį. Apsaugos sistemos saugo mūsų namus ir įspėja kaimynus arba policiją apie galimus įsilaužėlius. Finansinis saugumas – tai tinkamas investicijų paskirstymas, tikintis, kad investuotos lėšos augs užtikrindamos saugią ateitį. Kiekvienas iš šių terminų turi labai specifinę reikšmę, atsižvelgiant į vartojimo kontekstą. Lygiai taip pat informacijos saugumo termino prasmė priklauso nuo to, kokį iš trijų svarbių informacijos saugumo aspektų analizuojame: konfidencialumą, vientisumą ir prieinamumą. Konfidencialumas užtikrina, kad informacija neprieinama neįgaliotiems asmenims. Vientisumas užtikrina teisėtus įgaliotų asmenų duomenų mainus. Prieinamumas leidžia įgaliotiems asmenims reikiamu laiku prieiti prie vertybių. Informacijos saugumas analizuoja šiuos tris tikslus. O vienas iš iššūkių, kuriant informacines sistemas, – rasti pusiausvyrą tarp dažnai tarpusavyje prieštaraujančių tikslų [2].

Organizacija, siekianti padidinti savo informacijos saugą užtikrinant minėtų tikslų apsaugą, privalo sukurti informacijos saugos valdymo strategiją, kuri jai padėtų apsaugoti nuo kylančių grėsmių tiek organizacijos viduje, tiek išorėje, surasti visas kritis ir kitas vertingas

organizacijos vertybes¹, bei pamatuoti kylančias joms grėsmes. Tik nustačius, surūšiavus ir išanalizavus visas vertybes galima potencialiai pasverti kylančią grėsmę jų neautorizuotam sunaikinimui ar kompromitavimui. Turto vertinimas suteikia pakankamą vaizdą vertinant realią riziką, susijusią su potencialiais šių vertybų pažeidžiamumais ir grėsmėmis [3]. Vertybų kainą ar grėsmių daromą žalą nusakyti skaitine reikšme galima iš dalies paprastai, tačiau nusakyti šios grėsmės mastą gali būti gana sudėtinga. Dauguma šiai laikais saugumui skirtų produktų turi sudėtingas valdymo sąsajas, kurios nesugeba pateikti išsamaus vaizdo apie visas organizacijai kylančias grėsmes. Tam i pagalbą galima pasitelkti vizualizaciją. Vizualizacija gali padėti saugumo analitikams, pasitelkus savo intelektą, įgūdžius ir kūrybiškumą priimti tinkamus sprendimus, parengti būtinus veiksmų planus, vykdyti ateities simuliaciją. Vizualizacija yra vienas iš būdų atvaizduoti esamą situaciją iš surinktos informacijos. Dėka vizualizacijos surinktus duomenis transformuojant i grafinę reprezentaciją analitikams leidžia paprasčiau ir greičiau apdoroti informaciją [4].

Didėjant informacinių technologijų apimtimi, tobulejant informacinių technologijų sprendimams, vizualizacijos technologijoms, vis daugiau informacijos saugos specialistų pasitelkdami vizualizaciją bando spręsti informacijos saugos suvaldymo problemą ir apsaugoti turimas vertybes nuo kylančių išorinių ir vidinų grėsmių.

Toliau šiame darbe bus analizuojamos šiuolaikinės vizualizacijos technologijos ir tiriami egzistuojantys šių technologijų saugos sprendimai, pagal pasirinktą informacijos saugos vertinimo metodiką atliekami tolesni darbai, siekiant sukurti novatorišką grėsmių vizualizavimo prototipą, kurį būtų galima pritaikyti informacijos saugos valdymo procese užtikrinant informacijos saugumo tikslus.

1.1. Tyrimo objektas

Tyrimo objektas, tai – grėsmių vizualizavimo metodai, kurie suteikia galimybę įvertinti įstaigos ar organizacijos informacijos saugą.

1.2. Darbo tikslas ir uždaviniai

Darbo tikslas – pagerinti informacijos saugos valdymo grėsmių atvaizdavimo metodus ir grėsmių vertinimą.

¹ Šiame darbe vertybėmis vadinama visa įstaigos ar organizacijos programinė ar aparatinė įranga, žmogiškieji ištekliai, ar kita įranga, kuri turi savo vertę.

Uždaviniai:

1. išanalizuoti vizualizacija paremtų saugos sistemų projektus ir šiuolaikines vizualizacijos technologijas;
2. atliki grėsmių vizualizavimo panaudojimo probleminės srities analizę;
3. pasiūlyti metodą grėsmių vizualizavimo taikymui informacijos saugos valdymo įgyvendinimui;
4. įgyvendinti pasiūlytą metodą: sukurti prototipą ir jį išbandyti.

1.3. Temos naujumas

Kompiuterinė grafika nuo atsiradimo pradžios buvo naudojama mokslinių problemų tyrinėjimams, tačiau pirmosiomis savo dienomis prasta grafikos kokybė ribojo jos naudą. Platesnio dėmesio vizualizacija sulaukė 1987 metais paskelbus straipsnį „Vizualizacija mokslinėje kompiuterijoje“ žurnale „Kompiuterinė grafika“ [5]. Pastarajį dešimtmetį sparčiau vystantis ir tobulėjant kompiuteriniams įrenginiams vizualizacijos pritaikymas įvairiuose sprendimuose tampa daugiau prieinamas, todėl kompiuterinės 3D vizualizacijos taikymą galime laikyti šiuolaikiška temą.

Šiame moksliniame darbe informacijos saugos valdymui užtikrinti bus pasitelkta 3D įstaigos ar organizacijos vertybių vizualizacija, kuri pasaulyje dar nėra plačiai naudojama saugos sprendimuose siekiant trimatėje erdvėje apibrėžti turimų vertybių geolokaciją ir kylančių grėsmių ir rizikos laipsnio pagal atitinkamą spalvų skalę atvaizdavimą siekiant užtikrinti rizikos valdymą bei analizuoti veiklos rezultatus saugumo srityje.

1.4. Temos aktualumas

Temos aktualumą lemiantys veiksnių:

- lankstūs, paprasti bei funkcionalumo praplėtimo galimybę turintys saugumo sprendimai yra populiarūs ir jeigu jie „veikia“, tada visada suras savo nišą;
- vizualizacijos pritaikymas leidžia lengviau ne tik saugumo analitikams, bet ir mažai saugumo srities žinių turintiems asmenims susidaryti nuomonę apie susidariusią saugumo situaciją įstaigoje ar organizacijoje;
- galimybė dokumentaciją pateikti su grafine medžiaga suteikia didesnį įspūdį, daugiau papildomos informacijos, kuri leidžia greičiau susiorientuoti esamoje situacijoje;

- grėsmių vizualizacija paremta sistema galėtų naudotis kiekviena įstaiga ar organizacija, kuri šalia savo saugos sprendimų galėtų naudoti grėsmių vizualizavimo prototipą leidžiantį lygiagrečiai užtikrinti vertybių ir informacijos saugos valdymą, vizualizuoti vertybėms kylančias grėsmes, kurias pateiktų rizikos valdymo rezultatų ataskaitoje.

1.5. Tyrimo metodika

Analitinėje dalyje taikomi mokslinės literatūros, įvairių dokumentų, statistinių duomenų analizės ir informacijos apdorojimo metodai. Grėsmių vizualizacijos sistemos prototipui projektuoti naudojami loginiai, sistemų projektavimo ir modeliavimo metodai. Igyvendinant grėsmių vizualizacijos sistemos prototipą taikomi programavimo, tyrimų ir eksperimentiniai metodai.

1.6. Mokslinė darbo vertė

Iš mokslinio darbo rezultatų galima nusakyti, kokiuose šiuolaikiniuose saugumo sprendimuose pritaikoma vizualizacija, daryti išvadas, kaip vizualizacija padeda spręsti informacijos saugumo problemas. Darbo pabaigoje bus pristatytas produktas – informacijos saugumo valdymo informacinės sistemos prototipas su įstaigos vertybėms kylančių grėsmių vizualizacijos galimybe. Tokį produktą gali naudoti bet kuri įstaiga ar organizacija, kuri siekia efektyviai valdyti savo turimas vertybes ir užtikrinti jų saugumą atliekant rizikos valdymo procedūras. Šio produkto funkcionalumą galima lengvai praplėsti naujas papildomais saugos sprendimais, pavyzdžiui grėsmių vizualizavimo metodas, kuris pagal informacijos saugumo specialisto rizikos vertinimą atvaizduoja pasirinkto objekto² vertybes ir jas vizualizuojatitinkamomis spalvomis pagal vertybėms kylančių grėsmių kritiškumą.

Grėsmių vizualizavimo metodas suteiks galimybę valdyti įstaigos objektuose esančių vertybių geolokaciją ir pasitelkiant geografinę grėsmių vizualizaciją pagal atitinkamą vertybių kritiškumą ir spalvų skalę atvaizduoti įstaigos ar organizacijos vertybėms kylančias grėsmes ir rizikas.

1.7. Darbo rezultatai

Darbo metu yra gauti tokie rezultatai:

² Šiame darbe objektu vadinama bet kokia tam tikro dydžio patalpos erdvė, kurią galima rasti pasirinktame įstaigos ar organizacijos pastate, statinyje, teritorijoje, ar kita.

- Egzistuojančių grėsmių vizualizacijos projektų ir šiuolaikinių vizualizacijos technologijų analizė parodė, kad egzistuoja panašių vizualizacijos sprendimų, kurie leidžia vizualizuoti tinklo įrangai kylančias grėsmes, tačiau nėra saugos sprendimų, kurie vizualizuotų 3D plokštumoje įstaigos ar organizacijos objektuose naudojamas vertėbes ir šiose vizualizacijose atitinkama spalvų skale atvaizduotų kylančių grėsmių ir rizikų kritiškumą. Dauguma panašių sprendimų yra sudėtingi, brangūs ir reikia specialiai tik tai užduočiai atlikti apmokyto informacijos saugumo personalo.

- Vizualizavimo panaudojimo probleminės sritis analizė parodė, kad grėsmių vizualizacija naudojama siekiant geriau suprasti įstaigai ir jos vertybėms galinčią kilti riziką, greičiau priimti tinkamus sprendimus kontrpriemonių klausimu ir apsaugoti turimas vertėbes nuo kylančių išorinių ir vidinų grėsmių.

- Pasiūlytas metodas grėsmių vizualizavimo taikymo informacijos saugos valdymo procese pagal kurį buvo projektuojamas grėsmių vizualizavimo prototipas. Grėsmių vizualizavimo metodas:

- apjungia vertėbių priežiūrą atliekančio personalo darbą su įstaigos ar organizacijos saugos specialistų darbu, kuriems yra teikiami naujausi vertėbių geolokacijos duomenys. Šie duomenys pagal įstaigos ar organizacijos vardu dirbančio saugos specialisto poreikių naudojami vertinant vertybėms kylančią riziką ir vizualizuojant šių vertėbių būvimo vietą atitinkamame objekte;

- suteikia galimybę vizualizuoti 3D plokštumoje įstaigos vertybėms kylančias grėsmes ir rizikas panaudojant atitinkamą spalvų skalę kylančių grėsmių ir rizikų kritiškumui nurodyti;

- leidžia analizuoti saugumo situaciją laiko ašyje, spausdinti ataskaitas su vertybėms kylančių grėsmių ir rizikų vizualizacijomis, kurios leidžia pagreitinti saugumo klausimų sprendimo priėmimą ir padidinti atliekamo rizikos valdymo efektyvumą;

- naudoja tarptautinėje erdvėje pripažintą NIST rizikos valdymo metodologiją 800-30.

- Pasiūlyto metodo įgyvendinimui sukurtas prototipas ir atlikti bandymai parodė, kad metodas pagerina informacijos saugos valdymo grėsmių vertinimą. Siūlomas grėsmių vizualizavimo prototipas:

- pagal atitinkamą spalvų skalę vizualizuojant įstaigos vertybėms kylančias grėsmes ir rizikas 3D plokštumoje, laiko ašyje leidžia stebėti priimtų saugos sprendimų

efektyvumą ir kylančių rizikų pokyčių istoriją, formuoja rizikos valdymo ataskaitas PDF formatu;

- naudoja RBAC prieigos kontrolę, kuri leidžia pagal įstaigos ar organizacijos darbo pobūdį darbuotojams priskirti atitinkamus prototipo vaidmenis, todėl personalui paskirtomi tik tie darbai už kuriuos jie turi būti atsakingi;
- naudojasi šiuolaikinėmis vizualizavimo technologijomis siekiant išspresti įstaigos ar organizacijos nuolat kintančioje aplinkoje saugumo valdymo problemą;
- leidžia analizuoti veiklos rodiklius diegiant kontrpriemones ir mažinant įstaigos ar organizacijos vertybėms kylančią grėsmę ir riziką.

1.8. Darbo struktūra

Pirmame skyriuje yra apibrėžiamā nagrinėjama problema ir pasiūlomas jos sprendimo būdas, nusakomas nagrinėjamas objektas, pateikiamas darbo tikslas ir uždaviniai, apibūdinama numatoma nagrinėti tema pabrėžiant jos naujamą ir reikalingumą, taip pat aprašoma naudojama tyrimo metodika, mokslinio darbo vertė ir gauti rezultatai.

Antrame skyriuje yra analizuojami egzistuojantys vizualizacijos saugos sistemų sprendimų projektais, su informacijos saugos valdymu susijusi literatūra ir vizualizacijos technologijos.

Trečiame skyriuje analizuojama grėsmių vizualizacijos panaudojimo informacijos saugumo valdyme problematiką, aprašomas siūlomas grėsmių vizualizacijos metodas.

Ketvirtame skyriuje aprašomas siūlomo metodo realizavimas, vartotojo sasajos reikalavimai, funkciniai ir nefunkciniai programų sistemos reikalavimai, atliekami grėsmių vizualizacijos bandymai.

Penktame skyriuje pateikiama išvados ir tolimesni darbai.

Šeštame skyriuje pateikiama literatūros sąrašas.

1.9. Darbo aprobatacija

Svarbiausieji darbo rezultatai pagal tezių tematiką pateikti 2015 m. balandžio 16 dienos pranešime, skaitytame Vilniaus Gedimino technikos universitete vykusioje 18-ojoje jaunujų mokslininkų konferencijoje.

2. Susijusios literatūros analizė

Atsižvelgiant į informacinių technologijų svarbų vaidmenį šiandienos verslui, informacijos saugumas turi būti vienas svarbiausių komponentų moderniam verslo planavimui ir valdymui [6]. Šiame skyriuje aptariamos problemos su kuriomis susiduria informacijos saugumo valdymas, ir kaip jas gali padėti išspręsti grėsmių vizualizacijos pritaikymas, taip pat vizualizacijos saugos sprendimai ir vizualizacijos technologijos.

2.1. Informacijos saugumo valdymo problema

Šiandien įstaigos kartu su savo verslo partneriais ar klientais dirba per komunikacinius tinklus, tokius kaip internetas ar ekstranetas. Ten, kur vyksta duomenų mainai, patiriamas saugumo problemų. Bendras informacijos saugumo tikslas – stiprinti pasitikėjimą ir informacinių paslaugų efektyvumą įstaigoje arba tarp įstaigos ir jos išorinių verslo partnerių [7].

Informacijos saugumo valdymas apsaugo visą vertingą informacinių turta ir mažina įvairias jam kylančias rizikas, kurios atsiranda iš įvairių įstaigos aplinkos pusės taikant saugumo technologinius sprendimus ir valdymo procesus [6]. Siekiant mažinti turtui kylančias rizikas būtina nustatyti kokios grėsmės jas sukelia ir atitinkamai atliglioti rizikos mažinimą. Prastas grėsmių rimtumo matomumas ir laipsnis, pagal kurį rizikos ir kylančios grėsmės yra efektyviai mažinamos, yra daugiametė saugumo problema, kuri sukelia daugiau problemų kiekvienam bandančiam suvokti dabartinę informacijos saugumo būklę [8]. Interaktyvi vizualizacija panaudojant grėsmių kritiškumą nusakančias spalvas leistų geriau suvokti informacijos saugumo būklę.

Iš 2013 metų „PwC“ atliktos apklausos analizės rezultatų buvo iškirtos keturios kritinės sritys kurios turi didžiausią įtaką JAV įstaigų pasipriešinimui elektroniniams nusikaltimams:

- 1) Ekosistemos platumu suprasti galimas kilti rizikas;
- 2) Integruoti grėsmių paiešką ir informacijos pasidalijimą į aktyvią gynybos programą;
- 3) Nustatyti ir sumažinti elektroninius nusikaltimus įvykdytus patikimų saviškių;
- 4) Suprasti ir efektyviai naudoti kibernetinio saugumo technologijas [9].

Geriau suprantant šias sritis turėtų būti suteiktas įstaigų vadovams didesnis pagrindas pritaikant kibernetinio saugumo strategijas. Siekiant spręsti šias kritines sritis, įstaigoms būtina turėti rizikas sukeliančių grėsmių prevencijos programas. Tai gali būti ir sistema, kuri leidžia

realiu laiku stebėti turimas vertėbes ir matyti kokios grėsmės gali joms kilti ir atitinkamai jas įvertinti. Tokios sistemos prototipo sukūrimas bus vienas iš šio magistrinio darbo rezultatų.

Iš 2015 metų atliktos ISACA ir „RSA Conference“ informacijos saugumo specialistų apklausos su siekiu nustatyti esamą informacijos saugumo būseną galima išskirti, kad nors techninis ir administracinis reguliavimas gali padėti užkirsti kelią arba vilkinti daugelį apklausos metu pateiktų atakų tipų, dažniausiai žmogus yra didžiausia silpnybė. Mokinant žmones kaip aptikti ir reaguoti į galimas saugumo atakas yra plačiai manoma, kad sumažinamas tam tikros atakos vektorių efektyvumas [10].

Dauguma informacijos saugumo specialistų teigiančių, kad jų įstaigose sėkmingai yra vykdomos informacijos apsaugos sąmoningumo programos, sėkmingų atakų tipų išnaudojimo rezultate pasirodė prasčiau nei tie specialistai, kurie teigė, kad jų įstaigose nėra vykdomos informacijos apsaugos sąmoningumo programos. Tokius rezultatus galėjo lemti netinkamai rengiamos programos informacijos apsaugos sąmoningumui kelti, ar galimų atakų tipų atitinkamoms vertybėms keliamų grėsmių nuolat kintančioje informacijos apsaugos aplinkoje neapskaitomumas, netinkamas interpretavimas, ar kita. Kuriamame sistemos prototipe turėtų būti įgyvendinta galimybė matyti atitinkamų vertibių grėsmių sąrašus ir esant poreikiams juos praplėsti.

Teisinga sakyti, kad informacijos saugumas yra socialinė ir organizacinė problema, nes techninės sistemos turi būti valdomos žmonių. Vien geras saugumo sprendimas negali apsaugoti įstaigos be gero valdymo politikos ir jos įgyvendinimo. Informacijos saugumas yra pirmiausia ne techninė problema, bet verslo ar valdymo problema [11]. Tokiomis problemomis spresti galėtų būti naudojama sistema, kuri leistų plėtoti verslo planavimą ir valdymą lygiagrečiai kaupiant informaciją, susijusią su informacijos saugumu ar turimų vertibių kritiškumu, kas leistų užtikrinti pakankamą informacijos saugumą valdymo procese.

Su informacijos saugumu susiję moksliniai tyrimai neturėtų tik bandymais eiti į saugos sistemų ir technologijų technines detales, nes jos laikui bėgant keisis [12]. Prototipo sistema turėtų būti kuriamą atsižvelgiant į informacijos saugumo gerą praktiką naudojantis plačiai naudojama atitinkama rizikos valdymo metodologija. Vizualizacijos naudojimas suteiktu galimybę lengviau įvertinti vertibių kritiškumą ir esamą informacijos saugumo aplinką ne tik saugumo specialistams, bet ir įstaigos vadovams, kitam su informacijos saugumu nesusijusiam personalui.

2.2. Vizualizacijos saugos sistemų sprendimai

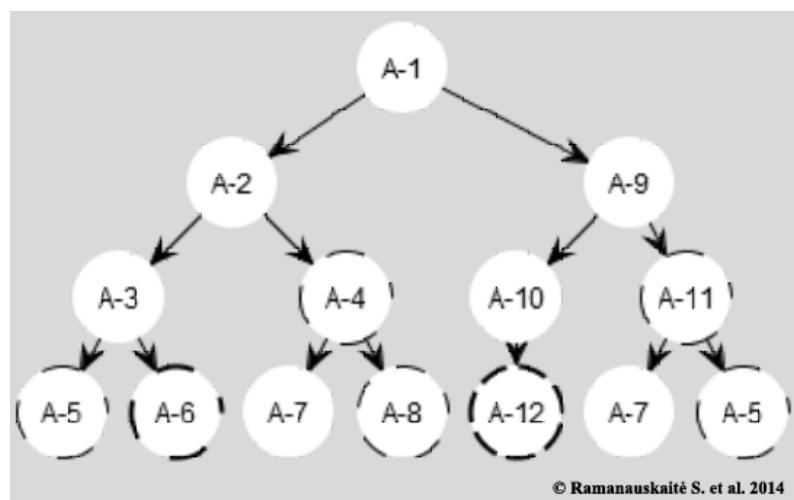
Analizuojamos vizualizacijos pritaikymo galimybės saugos sistemų sprendimuose ir panašios sistemos.

2.2.1. Saugumo standartų žymėjimo vizualizacija

S. Ramanauskaitė [13] pasiūlė kelis būdus, kaip būtų galima suderinti vienu metu naudojamus kelis saugumo standartus panaudojant vizualizaciją. Kadangi saugumo standartai gali skirtis vienas nuo kito, tuo pačiu metu gali būti naudojami keletas standartų, tai sukuria standartų persiklojimą ir konfliktines vietas dėl jų reikalavimų skirtumų. Siekiant tuo pačiu metu suderinti saugumo standartus būtina atlikti šių standartų harmonizaciją. Tam pasiekti pasirenkama adaptyvaus žymėjimo metodas, kuris automatiškai integruoja pasirinktus standartus naudojant dokumentų žymėjimą pasirinktam standartui. Siekiant sumažinti sudėtingumą ir daugelio dokumentų žymėjimo poreikį kaip pagrindas naudojama viena ontologija, kuri sužymi visus likusius standartus. Tai reikalaus tiek žymėjimo dokumentų, kiek yra standartų, kuriuos reikia integruti. Adaptyvaus žymėjimo technika leidžia apjungti visus kitus minimus harmonizacijos metodus bei leidžia pasinaudoti jų pranašumais.

2.2.1.1. Naudojant grafų struktūrą

S. Ramanauskaitė [13] panaudojusi adaptyvų žymėjimą sužymėjo tokius saugumo standartus: PCI DSS, ISO 27001, ISSA 5173 ir NISTIR 7621 pasiūlytai saugumo ontologijai. (žr. 1 pav.) pavaizduota minėtų standartų žymėjimas panaudojant grafų struktūrą. Medžio tipo



1 pav. Standartinė žymėjimo vizualizacija naudojant grafų struktūrą [13]

struktūra atvaizduoja standartus bei pagrindinės struktūros paveldėjimo nuorodas. Kitos nuorodos gali būti atvaizduojamos per mazgus ir analizuojamos detaliai peržiūrint atitinkamus

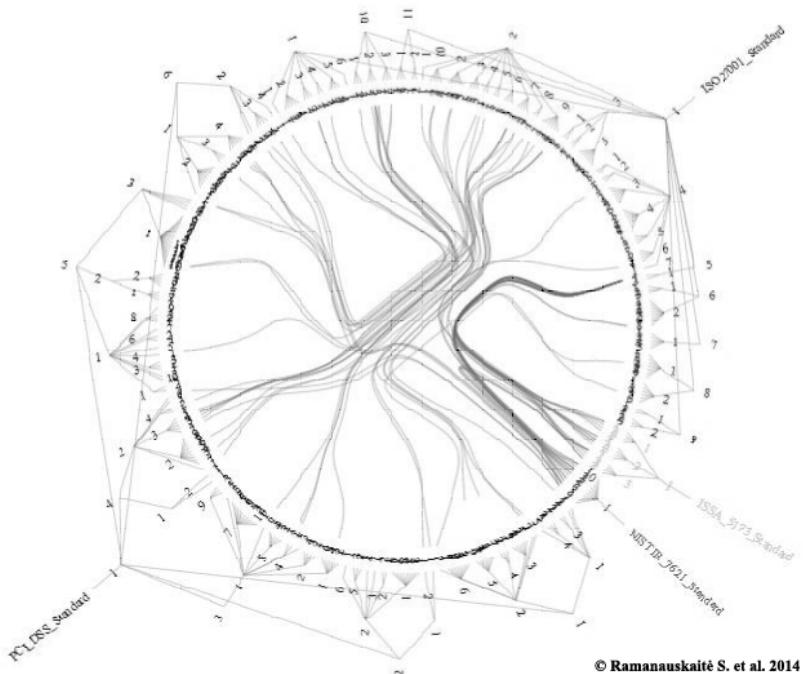
mazgus. Pasiūlytos mazgų užrašymo papildomas modifikuotas būdas sužymėtų standartų peržiūrėjimui:

- 1) mazgo linijos storis parodo kiek standartų turi analogus šiame kontrolės taške;
- 2) mazgo linijos forma atvaizduoja kaip standarto mazgas atitinka kitus standartus.

Kadangi saugumo standartai turi daug kontrolės taškų, tai šiam vizualizacijos stiliui reikia didelės peržiūros erdvės, kad visi taškai būtų atvaizduoti. Kitas įvardijamas trūkumas, tai galimybė vienu metu peržiūrėti tik vieną standartą, todėl nebus gaunama visa informacija kaip kiti standartai yra sužymėti vienas su kitu.

2.2.1.2. Naudojant „Chord“ diagramą

S. Ramanauskaitė [13] minėtiems standartams (žr. 2 pav.) pateikia pavyzdį naudojant pilną žymėjimą su „Chord“ centrine diagrama. Taip visi standartai ir jų kontroliniai taškai yra matomi vienoje diagramoje. Papildomai išoriniame žiede siūloma atvaizduoti standartų struktūras. Taip nors ir dydis šios diagramos bus didelis, tačiau bus pateiktas pilnas informacijos žymėjimas ir standartų struktūros.



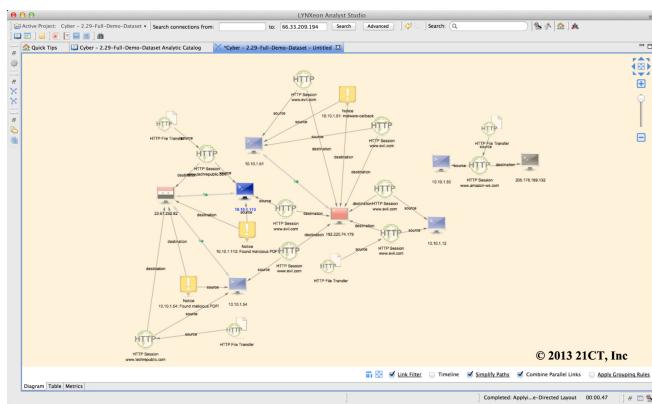
2 pav. Standartinė žymėjimo vizualizacija naudojant „Chord“ diagramą [13]

„Chord“centrinė diagrama gaunama apjungiant geriausias savybes kampinių rinkinių struktūros su supaprastinta centrinio rinkinio diagramos vizualia struktūros reprezentacija. Tam pirmiausiai apskaičiuojama klasterizuota nurodytos diagramos sluoksnio hierarchinė briauna, kuri sujungia kartu panašias briaunas. Po to atvaizduojami klasteriai vartotojo pasirinktame detaliajame lygyje naudojant naują nuotrauka paremtą techniką kuri apjungia atstumu paremtą

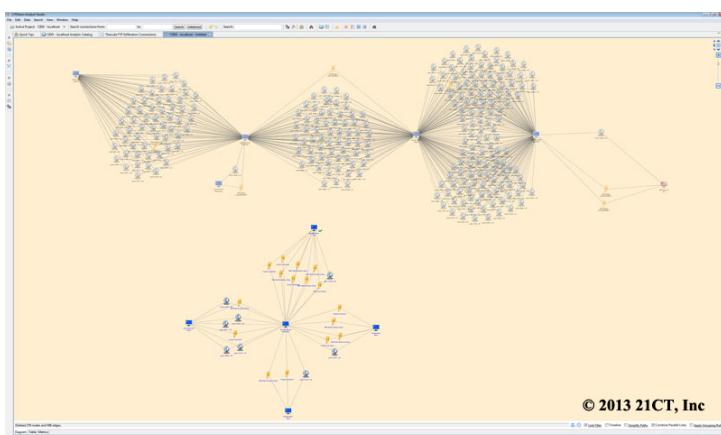
išskaidymą ir atvaizdo skeletizavimą. Galiausiai atvaizduojamas rezultatas kaip diagrama iš keletos mažų persidengiančių patamsintų briaunų rinkinių [14].

2.2.2. Saugumo analizė ir vizualizacija su „LYNNeon™“

Dauguma organizacijų naudojančių kompiuterių tinklo srauto stebėjimui naudoja statinių, signatūromis paremtų įspėjamasių sistemas. Pavyzdžiui dauguma organizacijų naudoja įsilaužimų detektavimo sistemos (IDS) arba įsilaužimų apsisaugojimo sistemos (IPS). Tačiau IDS ir IPS stebi tinklo srautą, kurį jis pažista arba mūsų nurodomas vykdytų atitinkamą stebėjimą. Trumpai tariant IDS ir IPS stebi tik tą srautą, kurį „pažista“ ir randa tas grėsmes, kurių signatūras jie turi. Tačiau kur lieka tinklo srautas, kurio niekas „neatpažista“? Tam reikia vykdyti pilną tinklo analizę. Vieną iš tokios analizės įrankių ir pristato „21CT“ kompanija, kuri platina „LYNNeon™“ analizės įrankį [15].



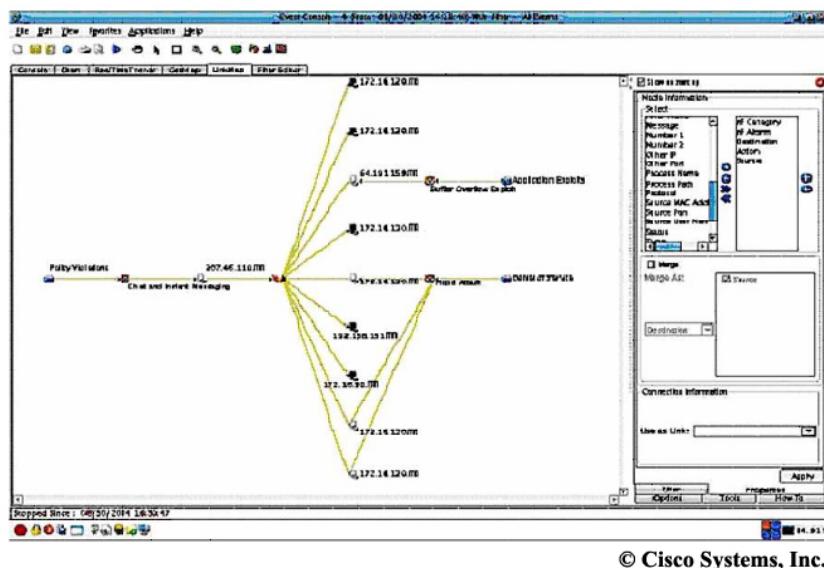
3 pav. Kenksmingo kodo paplitimo tinklo tyrimas [15]



4 pav. Tinklo vizualizacija [15]

2.2.3. Saugumo analizė ir vizualizavimas su „CiscoWorks“ SIMS

Saugumo informacijos valdymo sprendimas (SIMS) užtikrina eilę informacijos peržiūrą padedant saugumo analitikams identifikuoti grėsmes ir suprasti jų visas pasekmes. Analizei jis taip pat turi vizualizavimo įrankį, kurio pagalba užtikrinama aukšto lygio tinklo aktyvumo, paremto savais žurnaliniais nustatymais, peržiūra. Ši peržiūra leidžia dinamiškai nustatyti tam tikrus pažeidžiamumus tinkle [16].



5 pav. Tinklo vizualizacija [16]

2.2.4. Atakų vizualizavimas su CySeMoL

CySeMoL buvo sukurta siekiant modeliuoti SCADA sistemų architektūras. CySeMoL naudotojai gali modeliuoti savo kompiuterinius tinklus kaip įvesties duomenis naudodamiesi šioje kalboje aprašytomis bendrinėmis ir saugumo esybėmis. Modeliuojami įvesties duomenys yra pakeičiami saugumo skaičiavimo mechanizmu, kuris parodo atakos grafus su apytikslėmis sėkmingos atakos tikimybės reikšmėmis. Sėkmingas atakos tikimybės vertinimas atliekamas naudojantis Bajeso tinklais kartu su sąlyginių tikimybių formule [17].

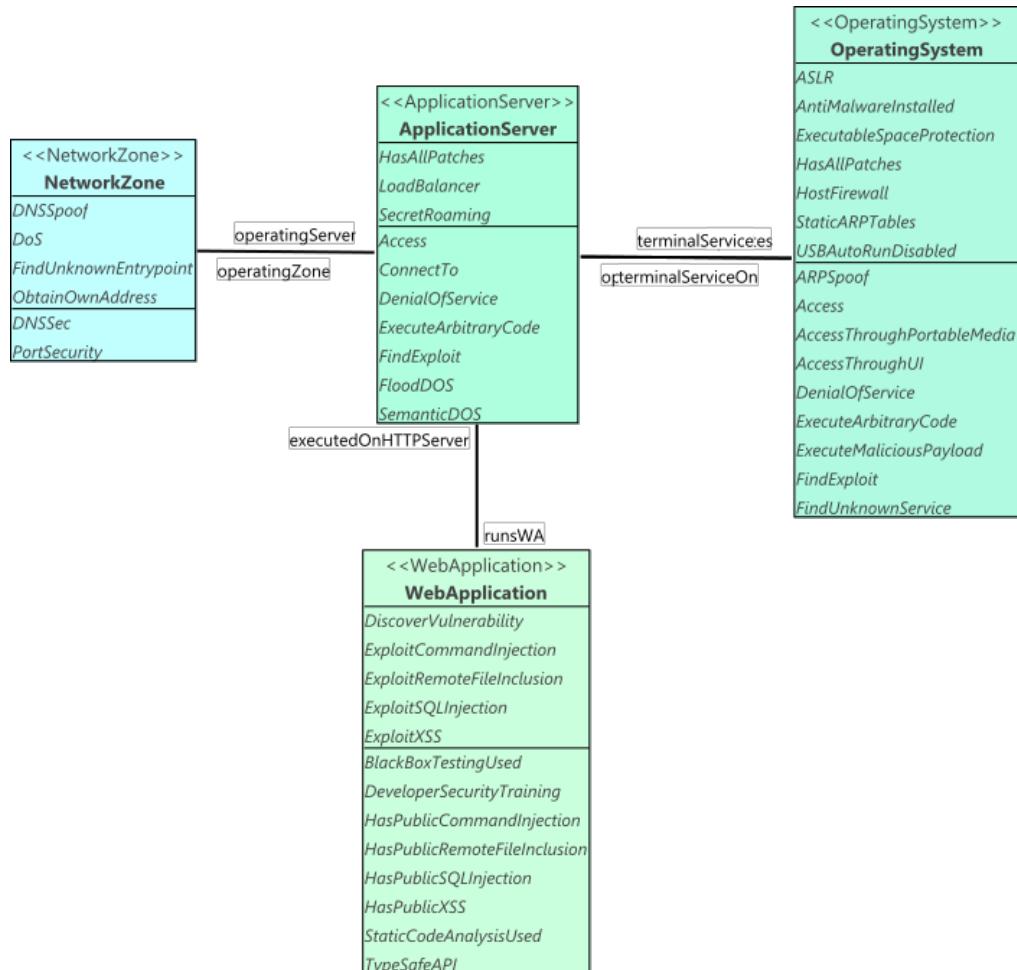
Bajeso tinklais galima susieti netiesiogiai susijusius kintamuosius. Bajeso tinklo „mazgai“ atstovauja kintamuosius, kurie gali arba negali būti tiesiogiai stebimi ir kuriuos paprastai būna sunku nuspėti, o „kraštai“ reiškia priežastinius arba įtakojančius sąryšius [18]. Bajeso tinklai lyginant su kintamaisiais, turinčiais tik po vieną bendrą paskirstytą sujungimą yra pranašesni, nes mažiau reikalauja atminties ištaklių, ypač jeigu yra naudojamas nedidelis grafas, o taip pat iš grafo yra lengviau suprasti kintamųjų sąryšius nei esant vienam dideliam kintamųjų paskirstymui. Šie tinklai naudojami daugumoje įvairių sričių, pavyzdžiui skaičiuojamojoje biologijoje, vaizdo apdorojime ir rizikos analizėje.

CySeMoL grafas nėra Bajeso tinklas, bet jis yra naudojamas grafo formavimui atliekant faktinius skaičiavimus. Kiekvienas mazgas CySeMoL grafe turi keletą požymių, kurie yra būdingi vienai iš dviejų kategorijų: „atakos žingsniui“ ir „gynybos“. Kiekvienas požymis yra Bajeso tinklo mazgas, o jų sąlyginės priklausomybės yra paremtos CySeMoL modeliu [19].

Pavyzdžiui CySeMoL (žr. 6 pav.) pateiktame pografijoje yra matomi 4 mazgai ir 3 kraštai. Skaičiavimo metu jie yra pakeičiami į Bajeso tinklą su 45 mazgais ir dar didesniu kiekiu kraštų.

Paruošęs objekto modelį CySeMoL naudotojas paleidžia skaičiavimo mechanizmą kurio pabaigoje, tikimybė, kad atitinkamas atakos žingsnis bus įvykdytas objekto modelyje vizualizuojamas naudojant spalvų skalę 0% (žalia) – 50% (geltona) – 100% (raudona). Didesnis procentas parodo didesnę tikimybę įvykdyti sėkmingą ataką [20].

Ryšiai tinkle priklauso nuo ankstesnių tyrimų ir domeno ekspertų vertinimų Cook`o metodu [21].



6 pav. CySeMoL modelio dalis

CySeMoL informacinių sistemų modeliavimą UML kalba apjungia su Bajeso atakų grafais vykdomais OCL kalboje [22]. CySeMoL kaip klasės modelis naudojamas kartu su EAAT objektinio modeliavimo programine įranga, kuri suteikia galimybę ją naudoti tiek modeliavimui, tiek analizei. CySeMoL klasės modelių funkcionalumą galima išplėsti naudojant klasės modeliavimo programinę įrangą.

2.3. Vizualizacijos technologijos

Vizualizacijos technologijos pasirinkimui tirsime, kokios vizualizacijos technologijos šiuo metu egzistuoja. Siekiant užtikrinti didesnę informacijos skliaidą pagrindinis dėmesys bus skirtas vizualizacijos technologijoms, kurios gali būti naudojamos uždaramame kompiuterių tinkle ar internete tarp nutolusių kompiuterio vartotojų.

Nagrinėjamos tokios technologijos kaip: „Adobe Flash“, HTML 5 „Canvas“, SVG, CSS, „JavaFX“, WebGL.

2.3.1. „Adobe Flash“

„Adobe Flash“ buvo sukurta 1996 metais, kuri suteikė galimybę atvaizduoti turtingą medijos turinį tinklalapiuose. Tuo metu 90-ujų viduryje dauguma tinklalapių buvo sudaryti iš statinių puslapių, kuriuose buvo atvaizduojamas tik tekstas ir nuotraukos. Kai atsirado „Adobe Flash“, jis atvėrė naują animacijos ir interaktyvumo galimybę internete. Žmonės galėjo kurti judančią animaciją ir paspaudžiamą interaktyvią grafiką, kuri viršijo HTML ir CSS standartines galimybes [23].

„Adobe Flash Player“ apdoroja „Adobe Flash“ programas, taip pat vadinamas SWF rinkmenomis. I „Adobe Flash Player“ turinys yra pristatomas interneto protokolu kaip instrukcijų rinkiniai dvejetainiame formate tiksliai aprašytame SWF rinkmenos formate. SWF rinkmenos paprastai yra talpinamos serveryje ir persiunčiamos, vaizduojamos kliento kompiuteryje jam užklausius. SWF rinkmenos susideda iš multimedijos turinio (vektorių, nuotraukų, garsų ir vaizdo įrašų) ir ActionScript instrukcijų. ActionScript, tai ECMA standartais paremta skriptinimo kalba naudojama „Adobe Flash“, kuri leidžia sukurti ir valdyti kliento pusėje naudotojo sąsajos elementus ir dirbtis su duomenimis. „Adobe Flash Player“ leidžia SWF rinkmenų turinį atvaizduoti plataus kiekio platformų, naršyklių ir įrenginių [24].

Keletas „Adobe Flash“ privalumų:

- Galimybė sukurti turtingą interaktyvią grafiką naudojant laiko juosta paremta PĮ įrankiu;

- Panaudoti pagalbines bibliotekas ir klasses kuriant sudėtingus projektus, kuriuos sukurti užstruktū ilgiau nei kuriant nuo nulio;
- Veikia vienodai tarp įvairių interneto naršyklių kaip „Internet Explorer“, „Mozilla Firefox“, „Opera“ ir „Chrome“;
- Gerai pritaikomas kurti duomenų intensyvioms animuotoms duomenų vizualizacijoms, kurias galima pasiekti internetu.

Keletas „Adobe Flash“ trūkumų:

- Neveikia daugybėje mobiliųjų išmaniuju prietaisų;
- Daugelis liečiamujų ekranų prietaisų, pavyzdžiui planšetiniai kompiuteriai, reikalauja skirtinį sąveikos galimybių, kurių „Adobe Flash“ dažniausiai nepalaiko;
- Neatitinka atvirų standartų interne, kuriuos yra apibrėžęs „W3C“ konsorciumas, neskatina standartizuoti atvirą internetą;
- Problemos susijusios su neįgaliesiems prieinamu turiniu interne naudojantis specialiais įrankiais, pavyzdžiui ekrano skaitytuval;
- Intensyvi „Adobe Flash“ grafika gali greitai išeikvoti daugumos nešiojamujų kompiuterių ir išmaniuju mobiliųjų įrenginių bateriją;
- Nesuderinama su SEO. „Adobe Flash“ tinklalapiuose yra pateikiama uždaros konstrukcijos, todėl sunku paieškos sistemoms juos indeksuoti [23]. Norint naudotis „Adobe Flash“ funkcionalumu reikalinga operacinėje sistemoje įdiegti „Adobe Flash Player“.

2.3.2. *HTML 5 „Canvas“*

HTML „Canvas“ žymė buvo įtraukta į HTML 5 rinkinį ir gali būti naudojama braižant grafinius elementus naudojant JavaScript. Pavyzdžiui tai gali būti panaudota grafų braižymui, nuotraukų kompozicijų kūrimui, animacijų sukūrimui arba net realaus laiko vaizdo apdorojimui ar atvaizdavimui.

„Canvas“ žymė gali būti naudojama WebGL atliekant aparatūros paspartintą 3D grafikos apdorojimą interneto tinklalapiuose. Šiuo būdu „Canvas“ elementas veikia 3D kontekste [25].

„Canvas“ elementas taip pat gali veikti 2D kontekste, naudojant plokščią Dekarto plokštumą, kurios pradžia (0,0) yra išsidėsčiusi viršutiniame kairiajame kampe, koordinačių erdvei slenkant į dešinę, kai x reikšmės didėja ir slenkant į apačią, kai y reikšmės didėja [26].

2.3.3. *SVG*

SVG yra dvimatę grafiką aprašanti kalba. Kaip atskiras formatas arba naudojant kartu su XML, ši kalba aprašoma XML sintakse, arba naudojant kartu su HTML 5 – HTML 5 sintakse. SVG leidžia trijų rūsių grafinius objektus: įvairias vektorines grafines formas kaip taškai sudaryti iš kreivų ir tiesių, nuotraukos ir tekstas. Grafiniai objektai gali būti sugrupuoti, stilizuoti, transformuoti ir sukompunuoti į anksčiau atvaizduotus objektus. Galimų funkcijų rinkinį apima sudėtinės transformacijos, kelių karpymai, alfa kaukės, filtrų efektais ir objektų šablonai.

SVG gali būti interaktyvi ir dinamiška. Jos animacija gali būti apibrėžta ir aktyvuota deklaratyviai, pavyzdžiui įdedant SVG elementus į SVG turinį, arba skriptais.

Galimos sudėtingos SVG programos naudojant papildomą skriptinimo kalbą, kuri pasiekia SVG DOM, kuris suteikia pilną priėjimą prie visų elementų, atributų ir savybių. Daug įvykių manipuliavimo galimų naudojant „onmouseover“ ir „onclick“ gali būti priskirti prie bet koks SVG grafinio objekto. Dėl savo suderinamumo ir įtakos su kitais interneto standartais skriptinimas su HTML ir SVG elementais gali būti vykdomas vienu metu ir tame pačiame interneto puslapyje [27].

2.3.4. *CSS*

CSS, tai kalba aprašanti interneto tinklalapių atvaizdavimą, įskaitant spalvas, maketus ir šriftus. Tai leidžia pritaikyti atitinkamą atvaizdavimą skirtingu rūsių prietaisams, turintiems didelius ekranus, mažus ekranus arba spausdintuvams. CSS yra nepriklausoma nuo HTML ir gali būti naudojama kartu su bet kokia XML žymėjimo kalba. HTML ir CSS atskyrimas leidžia lengvai atlikti svetainių priežiūrą, keisti stilius tarp tinklalapių ir pritaikyti tinklalapius įvairiomis aplinkomis. Taip yra vadina struktūros ar turinio atskyrimas nuo atvaizdavimo [28].

2.3.5. *JavaFX*

JavaFX klientinė platforma yra skirta turingo interneto turinio kūrimui ir jo atvaizdavimui daugumoje egzistuojančių įrenginių ir platformų. JavaFX yra visiškai integruota su „Java Runtime“, naudojasi „Oracle“ JRE teikiamu našumu ir pasauliniu mastu didelės įrenginių gausos, kuriuose ši aplinka yra įdiegta. JavaFX skatina produktyvią ir bendrą kūrėjo-dizainerio darbo eigą. JavaFX platforma turi esminį įrankių ir technologijų rinkinį, kuris kūrėjams ir dizaineriams suteikia galimybę bendradarbiauti, kurti ir diegti programas su išraiškingu turiniu naršyklėms ir kompiuteriams. Be to, mobiliųjų aplikacijų kūrėjai gali naudotis

integruotu emulatoriumi leidžiančiu peržiūrėti programas mobiliesiems ir televizijos įrenginams naudojantiems JavaFX platformą [29].

2.3.6. WebGL

WebGL yra nemokamas daugiaplatforminis interneto standartas žemo lygio 3D grafikos API paremtas OpenGL ES 2.0, veikiantis per HTML5 „Canvas“ žymę kaip DOM sąsają. Kūrėjai susipažinę su OpenGL ES 2.0 pripažysta WebGL kaip šešeliais paremtas API naudojantis GLSL su konstrukcijomis, kurios semantiškai yra panašios į tas pagrindines, kurios yra OpenGL ES 2.0 API. Jis lieka artimas OpenGL ES 2.0 specifikacijai su kai kuriomis išlygomis, kurių tikisi kūrėjai iš atminties valdomų kalbų, tokiu kaip „JavaScript“.

WebGL be jokių įskiepių suteikia galimybę internete naudotis 3D vizualizacija, kurios funkcionalumas yra jau įdiegtas interneto naršykleje. Didžiųjų interneto naršyklių kūrėjai, tokie kaip „Apple“ (Safari), „Google“ (Chrome), „Mozilla“ (Firefox) ir „Opera“ (Opera) yra WebGL darbo grupės nariai [30]. Šie nariai prisideda prie tolimesnės WebGL plėtrės.

WebGL privalumai:

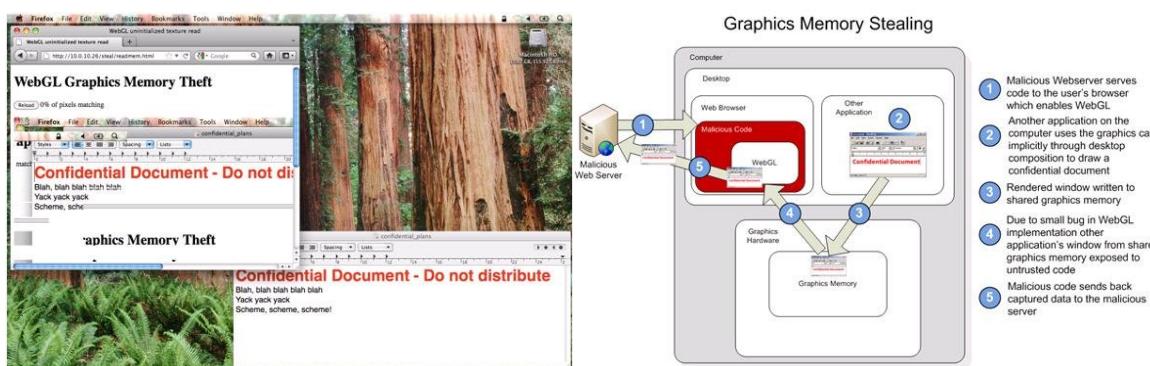
- galima atliliki užduotis, susijusias su grafiniu atvaizdavimu ir efektais, kurių negali atliliki su kitomis technologijomis kaip „Canvas“, SVG, „Adobe Flash“, „SilverLight“ ar kitos;
- palaiko naujosios interneto naršyklės, taip pat ir „Internet Explorer 11“;
- interneto naršyklėms nereikia jokių papildomų išplėtimų (angl. *plugins*), kaip „Java“, „Adobe Flash“ ar „SilverLight“.
- nepriklauso nuo naudojamos operacinės sistemos;
- palaikomas mobiliųjų įrenginių interneto naršyklėse „Windows Mobile“, „Opera“, „Firefox Mobile“ ir kitose;
- galima kurti šešelius (angl. *shaders*);
- integracija su DOM elementais, todėl yra galimybė kombinuotai taip pat naudoti CSS, SVG, „Canvas“;
- atviras standartas;
- pagrindinis naudojimas vizualizacijai, simuliacijai, žaidimams [31].

OpenGL ir kurios pagrindu kurta WebGL buvo kreipiamas didesnis dėmesys į greičio parametrus mažiau skiriant dėmesio saugumui. Šių technologijų panaudojimas turi potencialią saugumo riziką, bet jos dydį yra sunku įvertinti. WebGL saugumo šiuo metu daugiausiai rūpinasi

interneto naršyklų gamintojai, jie yra įdiegę tam tikrų saugumo sprendimų, skirtų apsaugoti WebGL, tačiau sunku įvertinti kaip šios apsaugos pasiteisins ateityje. Viena didžiausių rizikų, tai kad parašytas pirminis programos tekstas, kuris naudoja WebGL technologiją, yra tiesiogiai paleidžiamas kompiuterio naudotojo vaizdo kortoje ir gauna tiesioginę prieigą prie to kompiuterio vaizdo kortos API.

Dauguma vaizdo kortos taikomųjų programinių sąsajų iš pat pradžių buvo kuriamos ir naudojamos vietinių programų, kurios yra patikimos ir nebuvo manoma, kad ateityje bus naudojamos interneto naršyklėse. Todėl atsiranda susirūpinimas, ar savavališkos interneto svetainės nepradės atakuoti savo lankytojų sistemų.

Interneto naršyklėse bandoma pirminį programos tekštą tam tikru mastu talpinti į „Smėlio dėžę“ (angl. *Sandbox*), taip pat vykdoma eilė saugumo apribojimų, tokią kaip pažeidžiamų vaizdo kortų draudimas, atminties naudojimo apribojimai ir pataisos, kuriais užkertamas kelias kenkėjiškiems veiksmams [32].



7 pav. WebGL pažeidžiamumas ankstyvojoje išleidimo stadijoje [33]

2011 „Context“ pademonstravo kaip būtų galima pavogti vartotojo duomenis naudojant interneto naršykę panaudojant tuometinę „Mozilla Firefox 4“ WebGL implementaciją [33].

2.4. Vizualizacijos technologijos pasirinkimas

Vizualizacijos technologijos pasirinkimui atrinkti kriterijai pagal galimybes pasiekti užsibrėžtą tikslą ir sukurti novatorišką 3D grėsmių vizualizacijos metodą. Vienas iš pagrindinių reikalavimų – paprastas ir centralizuotas prototipo aptarnavimas ir prototipo patogumas naudotis jo teikiamu funkcionalumu eiliniam kompiuterio naudotojui.

1 lentelė. Vizualizacijos technologijų kriterijų lyginamoji lentelė

Kriterijus	Vizualizacijos technologija					
	„Adobe Flash“	HTML 5 „Canvas“	SVG	CSS	JavaFX	WebGL
2D vizualizacija	+	+	+	+ (ribota)	+	+
3D vizualizacija	+		+	+ (ribota)	+	+
Be interneto naršyklės papildomai nereikia diegti kitos programinės įrangos		+	+	+		+
Tinka naudoti sudėtingų formų vizualizavimui	+				+	+
Vizualizavimo sparta tinkama didelio objektų kiečio atvaizdavimui	+	+		+	+	+
Atvira specifikacija		+	+	+	+ (ribota)	+

Optimaliam naudojimui kompiuterių tinkle be papildomos programinės įrangos ir kaštų atžvilgiu įstaigos naudotojams efektyviausia būtų pasirinkti WebGL vizualizavimo technologiją, kuri taip pat yra suderinama su HTML 5 „Canvas“, JavaScript, SVG ir kitais atvirais formatais.

2.5. Antro skyriaus apibendrinimas ir pagrindiniai rezultatai

Analizuojant informacijos saugumo valdymo problemą pastebėtina, kad informacijos saugumo valdymo ir planavimo užtikrinimą lemia kritinis informacijos saugumo elementas – žmogus. Žmogus yra atsakingas ne tik už saugos sprendimų kūrimą, bet ir už tinkamą jų panaudojimą. Ne tik informacijos saugos specialistai yra atsakingi už įstaigos informacijos saugumą nuo išorinių ir vidinių grėsmių, bet ir visi toje įstaigoje dirbantys žmonės sąmoningai privalo tai užtikrinti. Tik tolygiai keliant socialinę sritį (įstaigos darbuotojų informacijos apsaugos sąmoningumas, kompetencija, kvalifikacija ar kita) kartu su organizacine sritimi (įstaigos informacijos apsaugos politika, procedūros, žinių bazė ar kita) bus galima išspresti informacijos saugumo problemą. Be viso to tinkamai nustačius galimas grėsmes (ypač kritines), kurios kelia ar potencialiai gali kelti įstaigos vertybėms riziką, ir atitinkamai jas sumažinant pasirenkus tinkamas kontrpriemones galima spręsti informacijos saugumo valdymo problemą. Šios problemas sprendimui galima pasitelkti grėsmių vizualizaciją, kuri leistų ne tik operatyviau reaguoti į kyylančias rizikas, bet ir atitinkamai užkardytį ar laiku pasiruošti šių rizikų užkardymui. Vizualizacija taip pat leistų įstaigų vadovams ar kitam su informacijos sauga nesusijusiam personalui geriau suvokti kylančią grėsmių kritiškumą ir atitinkamai priimti reikiamus sprendimus.

Analizuojant vizualizacijos saugos sistemų sprendimus S. Ramanauskaitės pasiūlyti būdai grafų struktūra ar „Chord“ diagrama galima perteikti saugumo standartų žymėjimą. Šiuos būdus būtų įmanoma panaudoti vizualizuojant informacijos saugos valdymo sistemų grėsmes, kurios gali kilti toms pačioms ar skirtingoms įstaigų vertybėms. „LYNNeon™“ ir „CiscoWorks“ SIMS įrankiai leidžia automatiniu būdu skenuojant kompiuterių tinklo srautą identifikuoti galimas grėsmes, tačiau šių įrankių negalima praplėsti ir jų funkcionalumas visiškai yra priklausomas nuo gamintojo leidžiamų atnaujinimų. Kuriant informacijos saugos sistemos grėsmių vizualizavimo prototipą pagrindinis dėmesys būtų skiriamas grėsmių vizualizavimo metodo galimybių praplečiamumui, o jo naudotojas pateikdamas įvesties duomenis turėtų visą jam suteiktą laisvę analizuoti įstaigos turimas vertybes, konfigūruoti nustatymus ir užtikrinti saugos veiklos rodiklius. Panašus vizualizacijos sprendimas – CySeMoL įrankis, kuris yra skirtas modeliuoti įvairias SCADA architektūras Bajeso tinklų pagalba leidžiantis vizualizuoti atitinkamų atakos žingsnių tikimybes panaudojant atitinkamą spalvų skalę. Kuriamas grėsmių vizualizavimo prototipas taip pat turėtų laisvai leisti naudotojui pasirinkti norimą spalvų skalę priklausomai nuo turimų rodiklių kritiškumo.

Analizuojant vizualizacijos technologijas WebGL kaip atviras standartas išskiria savo universalumu ir paprastumu, o lyginant su „Adobe Flash“ ir JavaFX, ji nereikalauja papildomų įskiepių ir programinės įrangos diegimo operacinėse sistemoje, yra daugiaplatforminis, kuris gerai veikia ir mobiliuosiuose įrenginiuose, ir yra palaikomas visų didžiujų interneto naršyklių kūrėjų. Kompiuterio vartotojui užtenka turėti interneto naršyklę su kuria gali gauti visą WebGL technologijos funkcionalumą. Atskirai HTML 5, SVG, ar CSS technologijos gali pasiūlyti tik ribotą vizualizacijos funkcionalumą 2D ar 3D kontekste, todėl nebūtų galimybės kurti novatyvų informacijos saugos valdymo grėsmių vizualizavimo prototipą, kuriame vizualizacija būtų pateikta 3D kontekste.

2.6. Antro skyriaus išvados

1. Atlikus informacijos saugumo valdymo problemos analizę, yra nustatyta, kad vizualizacijos panaudojimas gali pagerinti informacijos saugumo specialistams ar su informacijos sauga nesusijusiam personalui didesnį suvokimą apie įstaigoms kylančias grėsmes ir atitinkamai parinkti tinkamas kontrpriemones joms mažinti.
2. Atlikus vizualizacijos saugos sistemų sprendimų analizę, yra nustatyta, kad šiuo metu yra sukurta daug vizualizacija paremtų įrankių, kurie naudojami informacijos saugumui didinti, tačiau tik nedaugelis jų įstaigų vertybių valdymą yra integravę

nuolatiname informacijos saugos valdymo procese, pavyzdžiu kintant įstaigos vertybių būvimo vietai sistemoje iš karto matoma grėsmių geolokacijos, kurias sukelia šios vertybės, kaita.

3. Atlikus vizualizacijos technologijų analizę, yra nustatyta, kad kuriant sistemos prototipą efektyviausiai būtų galima panaudoti WebGL vizualizacijos technologiją.

3. Grėsmių vizualizavimo metodas

Grėsmių vizualizavimo prototipui sukurti bus naudojama Nacionalinio standartų ir technologijų instituto (NIST) specialaus leidinio 800-30 „Informacijos technologijų sistemų rizikos valdymo gairių“ rekomendacijų pagrindu sukurta rizikos valdymo metodologija. Grėsmių vizualizavimo prototipas rizikos valdymui užtikrinti bus grindžiamas pagal šiuos NIST rizikos valdymo metodologijos [34] etapus:

- 1) Sistemos charakterizavimas – pirmas etapas, kurio metu apibrėžiamos vertybės, pavyzdžiui programinė įranga, aparatinė įranga, personalas ir kiti duomenys, kurie įstaigai sukuria tam tikrą vertę;
- 2) Grėsmių identifikavimas – antras etapas, kurio metu peržiūrimi anksčiau įstaigoje įvykę atakų tipai ir sudaromas potencialių grėsmių, kurios gali kilti įstaigos vertybėms, sąrašas;
- 3) Pažeidžiamumų identifikavimas – trečias etapas, kurio metu peržiūrimi ankstesni rizikos vertinimai, auditorių pastabos, saugumo reikalavimai, saugumo testavimo rezultatai ir sudaromas potencialių pažeidžiamumų, kurie gali sukelti 2 etape identifikuotas grėsmes, sąrašas;
- 4) Apsaugos priemonių analizė – ketvirtas etapas, kurio metu identifikuojamos turimo ir planuoojamos įsigytis apsaugos priemonės (*paliekamas prie prototipo tolesnių darbų*);
- 5) Tikimybės nustatymas – penktas etapas, kurio metu įvertinama tikimybė grėsmės šaltiniui pasireikšti ir nustatomas dabartinė grėsmės tikimybės dydis įvertinant susijusių pažeidžiamumų kilmę ir šią tikimybę mažinančias kontrpriemonės;
- 6) Poveikio, kuris sukelia ar gali sukelti konfidencialumo, prieinamumo ar vientisumo praradimą, nustatymas – šeštas etapas, kurio metu atliekama poveikio analizė įvertinant įstaigos vertibių kritiškumą, duomenų kritiškumą ir jautrumą, nustatomas poveikio tam tikrai vertybei dydis;
- 7) Rizikos nustatymas – septintas etapas, kurio metu pagal grėsmės realizavimo tikimybės dydį ir poveikio vertybei dydį įvertinant turimų ir planuojamų kontrpriemonių adekvatumą nustatomi rizikos ir jų lygiai;
- 8) Rekomenduojamų kontrpriemonių nustatymas – aštuntas etapas, kurio metu stengiamasi sumažinti nustatytais rizikas iki priimtino lygio pasiūlant įdiegti papildomas kontrpriemones;

9) Rezultatų dokumentacija – devintas etapas, kurio metu formuojama rezultatų dokumentacija. Šiuo etapu pasibaigia rizikos valdymo procesas, kurio metu įvertinama kaip pasikeitė saugumo situacija įstaigoje ir numatomos ateities perspektyvos.

Ketvirtas NIST rizikos valdymo metodologijos etapas liks neįgyvendintas grėsmių vizualizavimo prototipe ir bus paliekamas tolesniems šio prototipo tobulinimo darbams.

Grėsmių vizualizavimo prototipas lyginant su kitais panašiais vizualizacijos saugumo sprendimais papildomai naudosis vaidmenimis grindžiama prieigos kontrole (RBAC). Vaidmenys yra kuriami įvairioms įstaigoms darbo funkcijoms, o naudotojams šie vaidmenys yra paskirstomi pagal jų atsakomybę ir kvalifikaciją. Naudotojai gali būti lengvai pakeisti iš vieno vaidmens į kitą [35].

Galima išskirti tokius prototipo pagrindinius vaidmenis:

1) Sistemos administratorius – šis vaidmuo suteikia teisę kurti naujas Grėsmių vizualizavimo prototipo naudotojus ir juos suskirstyti vaidmenimis, paskirstyti sistemos išteklius, keisti naudotojų prisijungimo duomenis, naikinti naudotojo sąsajas;

2) Vertybų priežiūros grupė – šis vaidmuo suteikia teisę sistemoje kurti naujas vertybes ir jas paskirstyti po įstaigos struktūrinius padalinius patalpos (objekto) tikslumu, pavyzdžiui IT skyriaus specialistams užtikrinti įstaigos tinklo įrangos paskirstymo priežiūrą ir administravimą (gali būti kelios grupės, kurios yra atsakingos tik už jiems priskirtas vertybes);

3) Informacijos saugumo grupė – šis vaidmuo suteikia teisę informacijos saugos specialistams pagal „Vertybų priežiūros grupių“ narių administruojamas įstaigos vertybes atliki informacijos saugos analizę, užtikrinti informacijos saugumo valdymą bei naudotis grėsmių vizualizavimo metodu.

Kaip vaidmenys atspindi organizacines pareigas ir funkcijas, taip vaidmenimis grįstas modelis tiesiogiai remia konkrečios įstaigos pasirinktą saugumo politiką. Buvo įrodyta, kad RBAC modeliai užtikrina „neutralią politiką“ t.y., naudojant vaidmenų hierarchijas ir apribojimus, gali būti išreikštose įvairios saugumo politikos, išskaitant ir įprastą ar vartotojo apibrėžtą DAC ir MAC prieigos kontrolę. Informacijos saugumo administravimas naudojant vaidmenis yra daug supaprastintas organizuojant prieigos teises [36].

RBAC suteikia pakankamai vertingą abstrakcijos lygi saugaus administravimo verslo įmonės lygmenyje, o ne vartotojo tapatybės lygyje.

Grėsmių vizualizavimo prototipe grėsmių vizualizavimo taikymo informacijos saugos valdymo proceso metodo įgyvendinimui ir įdiegimui bus naudojama WebGL vizualizavimo

technologija, kuri veiks HTML 5 „Canvas“ elemento ir „JavaScript“ kalbos pagrindu. „Vertybų priežiūros grupės“ narių administruojamas vertibes vertina „Informacijos saugumo grupės“ nariai pagal NIST rizikos valdymo metodologiją. Po kiekvieno vertinimo galutiniame rezultate automatiškai yra paruošiama įstaigos vertybų rizikos valdymo ataskaita. Pagal suformuotas įstaigos rizikos valdymo ataskaitas grėsmių vizualizacijai „Informacijos saugumo grupės“ nariai galės pasirinkti norimus įstaigos patalpas (objektus) ir automatiškai atitinkama spalva pagal nustatyta kritiškumą atvaizduos juose esančias vertibes. Pavyzdžiu (žr. 9 pav.) atvaizduota ta pati įstaigos vertybė turinti skirtingus rizikos laipsnius, t.y. mažas – žalia, vidutinis – geltona, didelis – raudona.



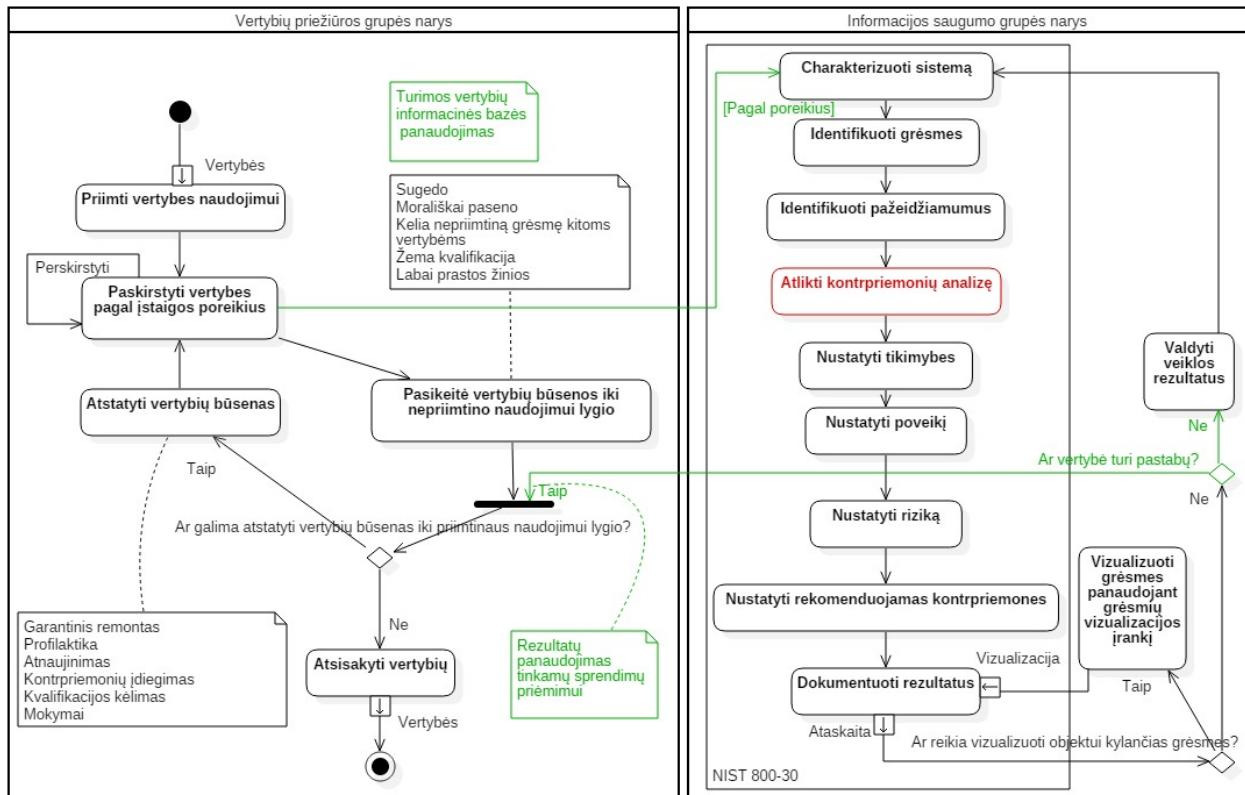
8 pav. Įstaigos vertybės rizikos laipsniai

Grėsmių vizualizavimo prototipas leis už vertibes atsakingiems įstaigos darbuotojams užtikrinti šių vertybų tinkamą priežiūrą ir administravimą, palengvins kasmetinę inventorizaciją, o informacijos saugos specialistams, kurie atsakingi už jiems paskirtų vertybų saugumą, suteiks naujausią informaciją apie įstaigos turimas vertibes ir jų buvimo vietą, kas leis pagerinti informacijos saugos rizikos vertinimą bei pagal kritiškumą vizualizuoti grėsmių įtakojamas vertybės pasirinktuose objektuose. Šiuo metodu įstaigos informacijos saugos veikla įtraukiamā į kasdieninę įstaigos darbo veiklą, kuri sumažina informacijos saugos vertinimo atlikimo laiką ir įveda saugos dokumentacijos automatizavimą kartu su papildomai įdiegta grėsmių vizualizavimo galimybe.

3.1. Grėsmių vizualizavimo metodo schema

Grėsmių vizualizacijos metodas, pagal kurį bus kuriamas prototipas, atvaizduotas UML veiklos diagramoje (žr. 9 pav.). Diagramoje vyrauja dviejų veikėjų sritys: Vertybų priežiūros grupės nario ir Informacijos saugumo grupės nario. Raudona spalva pažymėtas žingsnis, kurio

funktionalumas nebus įgyvendintas kuriant grėsmių vizualizavimo prototipą. Žalia spalva pažymėtas saryšis tarp nurodytų veikėjų sričių.



9 pav. Grėsmių vizualizavimo metodo schema

3.2. Grėsmių vizualizavimo metodo tekstinis aprašas

Pagrindiniai žingsniai naudojant grėsmių vizualizacijos metodą (žr. 9 pav.) pagal „Vertybų priežiūros grupės narį“:

1A Įstaigoje už vertybės atsakingas „Vertybų priežiūros grupės narys“ priima vertebes tolesniams jų disponavimui.

2A Vertybės pagal įstaigos poreikius yra paskirstomos ir esant naujiems poreikiams – perskirstomos po įstaigą ar kitus objektus. Grėsmių vizualizavimo prototipe ekspluatuojamų vertybų informacija naudojama inicializuojant sistemos rizikos vertinimą. „Informacijos saugumo grupės narys“ siekdamas įvertinti įstaigos informacijos saugumą pagal poreikius analizės tikslais gali pradėti įstaigos kylančių grėsmių ir rizikos vertinimą 1B.

3A Pasikeitus vertybų būsenai (pavyzdžiui sugedo kompiuteris) iki nepriimtino naudojimui lygio „Vertybų priežiūros grupės narys“ sprendžia, ar šios vertybės būseną įmanoma, galima ir

ar verta ją sugražinti į priimtiną lygi? Atsižvelgiant į kitų su nagrinėjamų vertybių valdymu susijusią asmenų pastabas (3b).

1a tuo atveju, kai nusprenčiama, kad galima ir verta atstatyti vertybių būseną į priimtiną lygi, vykdomas jų būsenos atstatymas ir gražinimas tolesniams paskirstymui įstaigoje.

2a tuo atveju, kai nusprenčiama, kad nėra galimybė, ar nėra verta atstatyti būseną į priimtiną lygi, vykdomas vertybės atsisakymas ir ji yra daugiau nebenaudojama.

Pagrindiniai žingsniai naudojant grėsmių vizualizacijos metodą (žr. 9 pav.) pagal „Informacijos saugumo grupės nari“:

1B „Informacijos saugumo grupės narys“ atlieka pasirinktos sistemos charakterizavimą panaudojant eksplotuojamų vertybių informaciją. Pasirinktos sistemos charakterizavimui taip pat naudojama patirtis igyta iš ankstesnių šios sistemos rizikos vertinimų.

Pastebėtina, kad informaciją sistemos charakterizavimui „Informacijos saugumo grupės narys“ gauna iš „Vertybų priežiūros grupės nario“ administruojamų duomenų 2A ir atlieka jos analizę.

2B Identifikuoja grėsmes, kurios gali kilti sistemai.

3B Identifikuoja pažeidžiamumus, kurie sukelia grėsmes.

4B Atlieka turimų kontrpriemonių analizę.

Pastebėtina, kad kontrpriemonių analizė nebus įgyvendinta grėsmių vizualizacijos prototipe, nes nėra šio darbo nagrinėjamos problemas objektas.

5B Nustato pažeidžiamumo sukeltos grėsmės tikimybę.

6B Nustato pažeidžiamumo sukeltos grėsmės poveikį (žalą).

7B Nustato ir įvertina galimą pažeidžiamumų sukeltų grėsmių riziką.

8B Nustato rekomenduojamas kontrpriemones.

9B „Informacijos saugumo grupės narys“ dokumentuoja visus savo rezultatus ir parengia ataskaitą, jos papildymui „Informacijos saugumo grupės narys“ sprendžia, ar jam reikia panaudoti grėsmių vizualizavimo metodą ir vizualizuoti įstaigos objektui kylančių grėsmes ir jų kritiškumą.

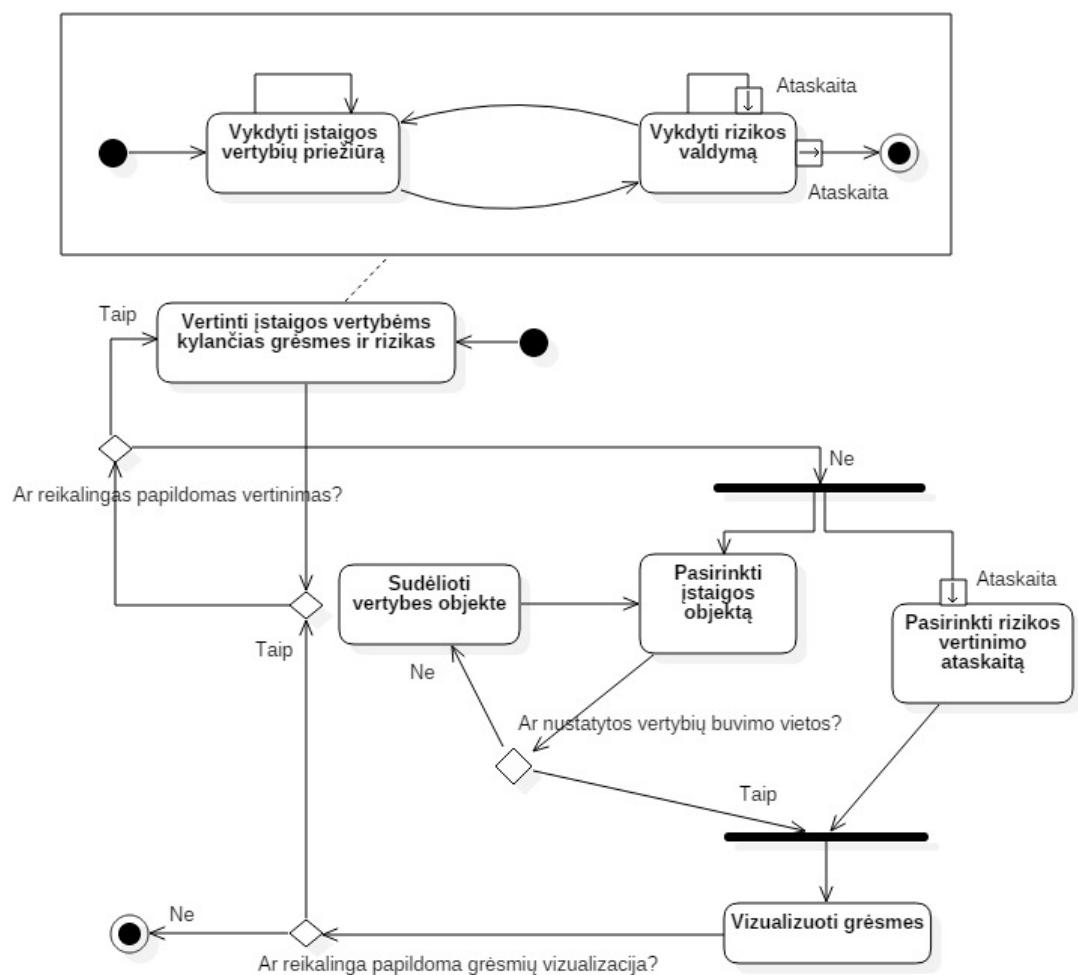
1b tuo atveju, kai nusprendžiama panaudoti grėsmių vizualizavimo metodą atliekamas grėsmių vizualizavimas, kurio rezultatai pagal poreikius įtraukiami į rizikos valdymo ataskaitą.

2b tuo atveju, kai nusprendžiama šio metodo nenaudoti pagal ataskaitos duomenis sprendžiami klausimai dėl įstaigos vertybių eksploatavimo (3A) siekiant sumažinti joms kylančias grėsmes.

3b atliekamas veiklos rezultatų valdymas, kurio metu vedama statistika, kaupiamą įgyta patirtis sekantiems rizikos vertinimams.

3.3. Grėsmių vizualizavimo eksplikacijos schema

Siūlomo metodo grėsmių vizualizavimo eksplikacija detalizuoja kaip bus panaudojamas prototipo vizualizavimo įrankis leisiantis sėkmingai atvaizduoti įstaigos vertybėms kylančias grėsmes ir rizikas 3D plokštumoje, o šios eksplikacijos žingsniai atvaizduoti UML veiklos diagramoje (žr. 10 pav.).



10 pav. Grėsmių vizualizacijos metodo eksplikacijos schema

3.4. Grėsmių vizualizavimo eksplikacijos tekstinis aprašas

Siūlomo metodo grėsmių vizualizavimo eksplikacijos (žr. 10 pav.) žingsniai:

- 1 Atliekamas įstaigos vertybių kylančių grėsmių rizikos vertinimas.
- 2 Sprendžiamas klausimas, ar reikia papildyti vertinimą su naujais duomenimis?

Pastebėtina, kad šis žingsnis susideda iš dviejų veikėjų darnaus darbo, t.y. vertybių priežiūros ir rizikos vertinimo (žr. 9 pav.).

1 tuo atveju, kai nusprendžiama, kad reikia papildyti kylančių grėsmių rizikos vertinimą, tada vykdomas šio vertinimo papildymas arba atliekamas naujas vertinimas su kitais parametrais.

2 tuo atveju, kai nusprendžiama, kad nereikia papildyti kylančių grėsmių rizikos vertinimo, tada pagal poreikius renkamasi konkretų įstaigos objektą, kurio grėsmių vizualizaciją siekiama atlkti. Vizualizacija bus atliekama remiantis prieš tai įvykdytu rizikos vertinimu.

3 pasirenkant įstaigos objektą sprendžiamas klausimas, ar visos vertybės esančios pasirinktame objekte turi nustatytas buvimo vietas?

1 tuo atveju, kai nusprendžiama, kad ne visų vertybių buvimo vietas yra apibrėžtos vykdomas vertybių buvimo vietas objekte nustatymas po kurio atnaujinimo grįztama į įstaigos objekto pasirinkimo langą.

2 tuo atveju, kai nusprendžiama, kad visos rūpimų vertybių vietas yra nustatyotos pasirenkama rizikos valdymo ataskaita su parengta rizikos vertinimo dalimi.

3 pagal atliktus pasirinkimus atliekama įstaigos objekto grėsmių vizualizacija su kuria vėliau galima papildyti ataskaitą. Sprendžiamas klausimas, ar reikia papildomai atlkti grėsmių vizualizaciją pasirenkant kitą objektą arba rizikos vertinimą?

3 tuo atveju, kai nusprendžiama, kad reikia atlkti papildomą grėsmių vizualizaciją grįztama prie 2. žingsnio nusprendžiant, dėl kylančių grėsmių rizikos vertinimo tinkamumo ir galimybės jo papildymui.

4 tuo atveju, kai nusprendžiama, kad nereikia atlkti papildomos grėsmių vizualizacijos, tada grėsmių vizualizavimo metodas daugiau nebenaudojamas.

Pastebėtina, kad po aptariamio būdas užbaigiamo, išprastai, bet nebūtinai grįztama prie kylančių grėsmių rizikos valdymo ataskaitos rezultatų tolesnio nagrinėjimo.

3.5. Trečio skyriaus apibendrinimas ir pagrindiniai rezultatai

Siekiant informacijos saugos valdymo procese įgyvendinti grėsmių vizualizacijos galimybę pasiūlytas metodas (žr. 9 pav.) siekiant sukurti prototipą, kuris leistų vizualizuoti ištaigai kylančias grėsmes ir rizikas pagal metodo eksplikaciją (žr. 10 pav.).

Grėsmių vizualizavimo prototipui sukurti bus naudojama NIST specialaus leidinio 800-30 „Informacijos technologijų sistemų rizikos valdymo gairių“ rekomendacijų pagrindu sukurta rizikos valdymo metodologija.

Grėsmių vizualizavimo prototipe veiks RBAC, kuriame pagrindiniai veikėjai: „Sistemos administratorius“, „Vertybų priežiūros grupė“, „Informacijos saugumo grupė“. Sistemos administratorius atsakingas už kitų dviejų grupių sklandų darbą. Vertybų priežiūros grupės nariai atlieka jiems priskirtų vertybų priežiūrą ir administravimą. Informacijos saugumo grupė – analizuoją turimus veiklos rodiklius, vertina kylančių grėsmių riziką, užtikrina informacijos saugumo valdymą ir vizualizuoją ištaigos vertybėms kylančias grėsmes ir rizikas siekiant atkreipti ištaigos vadovybės didesnį dėmesį į susidariusią situaciją tam tikrame kritiniame ištaigos taške.

Grėsmių vizualizavimo įrankis pasinaudodamas grėsmių vizualizavimo metodu leidžia atvaizduoti ištaigos objektus, kuriuose ištaigos valdomos vertybės yra nuspalvintos pagal „informacijos saugumo grupės“ nario nustatytais rizikos laipsnius, kuris apskaičiuojamas grėsmės tikimybės dydį dauginant iš galimo pažeidžiamumo dydžio (žr. 8 pav.).

Metodo įgyvendinimui apsispręsta panaudoti WebGL vizualizavimo technologiją paremtą HTML5 „Canvas“ elemento ir „JavaScript“ kalbos funkcionalumu.

Iš pasiūlyto metodo eksplikacijos diagramos (žr. 10 pav.) matyti, kad sėkmingam grėsmių vizualizavimo įrankio panaudojimui reikalinga: apibrėžti ištaigos objekte esančių vertybų buvimo vietas ir turėti paruoštą rizikos valdymo ataskaitos vertinimo dalį.

3.6. Trečio skyriaus išvados

Atlikus grėsmių vizualizavimo taikymo informacijos saugos valdymo procese metodo įgyvendinimo analizę yra nustatyta šio metodo įgyvendinimui panaudoti RBAC naudotojų vaidmenų atskyrimui, NIST rizikos valdymo metodologiją informacijos saugos valdymo

užtikrinimui, nutarta pagal grėsmių vizualizavimo metodo eksplikaciją kurti grėsmių vizualizavimo įrankį, kurio veikimas pavaizduotas paveiksle (žr. 10 pav.), taip pat sukurti prototipo informacinę sistemą į kurią būtų įdiegtas minimas įrankis. Kuriamo prototipo veikimas pagrįstas metodu, kuris pateiktas paveiksle (žr. 9 pav.). Pasiūlytas metodas leis valdyti įstaigos vertybių geolokaciją ir pagal vertybėms kylančią riziką vizualiai 3D plokštumoje atvaizduoti vertybių kritiškumo lygi.

Sukurto prototipo galutinė versija bus pristatyta Lietuvos Respublikos Nacionalinei komunikacijų apsaugos tarnybai ir Saugumo priežiūros tarnybai, ir aptarta galimybė pritaikyti ar panaudoti šį prototipą valstybinio sektoriaus įstaigų vertybių ir rizikos valdymo optimizavimui.

4. Grėsmių vizualizavimo metodo realizacija, bandymų atlikimas

Šiame skyriuje pagal 3. skyriuje pasiūlytą grėsmių vizualizavimo metodą bus atliekamas prototipo įgyvendinimas, t.y. vykdomas reikalavimų nustatymas, projektavimas ir kūrimas bei atliekami bandymai.

4.1. Grėsmių vizualizavimo prototipo reikalavimų specifikacija

Poskyryje detaliai nagrinėjami grėsmių vizualizavimo prototipo vartotojo sąsajos reikalavimai, funkciniai ir nefunkciniai informacinės sistemos reikalavimai.

4.1.1. Vartotojo sąsajos reikalavimai

4.1.1.1. Dalykinės srities metaforos reikalavimai

DSMR-1 *Vertybė* – tai savybė, kuri turi, ar duoda naudą.

DSMR-2 *Inventorius* – tai vertybė, kuri yra naudojama pagal jos paskirtį.

DSMR-3 *Istaiga* – teisiškai legitimus ir aiškią struktūrą turintis darinys siekiantis savo pagrindinio tikslą ir, kurį paprastai sudaro vadovybė ir jai pavaldūs padaliniai.

DSMR-4 *Objektas* – tai mažiausia įstaigos erdvės vienetas, vertybų buvimo vieta, pavyzdžiui kabinetas ar kita patalpa.

DSMR-5 *Grėsmių vizualizavimo prototipas* – tai interneto technologija grindžiama informacinė sistema, kurioje atliekama įstaigos vertybų priežiūra siekiant suvaldyti įstaigos informacijos saugumą, turi įdiegtą grėsmių vizualizavimo įrankį.

DSMR-6 *Grėsmių vizualizavimo įrankis* – įrankis, kuris leidžia stebeti įstaigos objekto vertybų kylančią grėsmių ir rizikos laipsnį.

DSMR-7 *Sistemos naudotojas* – įstaigos darbuotojas, kuris naudoja grėsmių vizualizavimo prototipo informacinę sistemą vykdymas savo įsipareigojimus ir darbo užduotis.

DSMR-8 *Sistemos administratorius* – sistemos naudotojas, kuris atlieka grėsmių vizualizavimo prototipo informacinės sistemos sprendimo priežiūrą ir yra atsakingas už šios sistemos naudotojų efektyvų ir veiksmingą darbą.

DSMR-9 *Vertybų priežiūros grupės narys* – sistemos naudotojas, kuris yra atsakingas už jam paskirtų įstaigos vertybų priežiūrą ir administravimą.

DSMR-10 *Informacijos saugumo grupės narys* – sistemos naudotojas, kuris yra atsakingas už įstaigos ir jos vertybų saugumą ir jų apsaugos organizavimą.

4.1.1.2. Formuluojamos užduotys

Grėsmių vizualizavimo prototipo sistema suteikia galimybę kurti sistemos vartotojų sąsajas (angl. *user interface*) pagal įstaigos poreikius. Sistemos administratorius valdo sistemos sąsajų kūrimą ir naikinimą bei gali suteikti ir atimti iš sistemos naudotojų sistemos techninius išteklius. Grėsmių vizualizavimo prototipe bus jau paruoštos tokios sistemos naudotojų vartotojo sąsajos turinčios tik sau būdingą funkcionalumą: sistemos administratorius, informacijos saugumo grupė, vertybų priežiūros grupė. Grėsmių vizualizavimo prototipo vartotojo sąsajos pateiktos priede A.

Grėsmių vizualizavimo prototipo sistemos reikalavimų užduotyse (GVSRU) bus nagrinėjami tik dalykiniuose reikalavimuose (DR) apibrėžtos užduotys, pagalbinės sistemos funkcijos yra nenagrinėjamos.

4.1.1.3. GVSR-1 vartotojo sąsajos užduotys

GVSRU-1 Užduotis „Patvirtinti sistemos naudotojo tapatybę“ pagal GVSR-1 vartotojo sąsają užtikrina DR-1 reikalavimo įgyvendinimą. Šią užduotį vykdo visi sistemos naudotojai, kurie siekia prisijungti prie sistemos arba pasibaigus sesijos laikui per naują nori naudotis sistemos funkcionalumu.

2 lentelė. GVSRU-1 užduoties aprašas

Veiksmas	Komanda	Parametrai	Duomenys
Prisijungti prie sistemos	login(username, password)	Sistemos naudotojo prisijungimo vardas ir slaptažodis	Nukreipimas į pirmą, pagal sistemos naudotojo turimas teises, meniu skyrių.

4.1.1.4. GVSR-2 vartotojo sąsajos užduotys

GVSRU-2 Užduotis „Vykdyti sistemos naudotojų administravimą“ pagal GVSR-2 vartotojo sąsają užtikrina DR-2 reikalavimo įgyvendinimą. Šią užduotį sistemos meniu skyriuje „Administratoriai“ vykdo sistemos administratorius siekdamas užtikrinti sistemos naudotojų nenutrūkstamą prieigą prie sistemos.

3 lentelė. GVSRU-2 užduoties aprašas

Veiksmas	Komanda	Parametrai	Duomenys
Peržiūrėti sistemos naudotojų sąrašą	listUsers()		Sistemos naudotojų sąrašas
Inicijuoti naujo sistemos naudotojo duomenų	addUser()		Sistemos naudotojo duomenys

įtraukimą į naudotojų sąrašą			
Patvirtinti naujo sistemos naudotojo įtraukimą į naudotojų sąrašą	addUser(Data)	Užpildyti formos duomenys	Galimas formos klaidų sąrašas ir sistemos naudotojo duomenys arba nukreipimas į sistemos naudotojų sąrašą
Inicijuoti sistemos naudotojo duomenų pakeitimą	editUser(userID)	Sistemos naudotojo identifikacinis numeris	Sistemos naudotojo duomenys
Patvirtinti pakeistus sistemos naudotojo duomenis	editUser(userID, Data)	Sistemos naudotojo identifikacinis numeris ir kiti užpildyti formos duomenys	Galimas formos klaidų sąrašas ir sistemos naudotojo duomenys arba atnaujinti sistemos naudotojo duomenys ir nukreipimas į sistemos naudotojų sąrašą
Ištrinti sistemos naudotojo duomenis	removeUsers(userID)	Sistemos naudotojo identifikacinis numeris	Sistemos naudotojų sąrašas

GVSU-3 Užduotis „Vykdinti įstaigų, jos struktūrinų padalinių ir objektų struktūrizavimą“ pagal GVSR-2 vartotojo sąsają užtikrina DR-3 reikalavimo įgyvendinimą. Šią užduotį sistemos meniu skyriuje „Įstaigos“ vykdo vertybų priežiūros grupės nariai siekdamai užtikrinti, kad būtų turima naujausia informacija apie įstaigų struktūrinius padalinius ir objektus.

4 lentelė. GVSU-3 užduoties aprašas

Veiksmas	Komanda	Parametrai	Duomenys
Peržiūrėti įstaigų sąrašą	institutions()		Įstaigų sąrašas
Įtraukti naują įstaigą į įstaigų sąrašą	institutions(Name)	Įstaigos pavadinimas	Nukreipimas į įstaigų sąrašą
Ištrinti įstaigos duomenis	removeInstitution(ID)	Įstaigos identifikacinis numeris	Nukreipimas į įstaigų sąrašą
Peržiūrėti struktūrinų padalinių sąrašą	listing()		Pilnas įstaigos struktūros sąrašas
Inicijuoti naujo struktūrinio padalinio duomenų įtraukimą į struktūrinų padalinių sąrašą	add()		Struktūrinio padalinio duomenys
Patvirtinti naujo struktūrinio padalinio duomenų įtraukimą į struktūrinų padalinių sąrašą	add(Data)	Užpildyti formos duomenys	Galimas formos klaidų sąrašas ir struktūrinio padalinio duomenys arba nukreipimas į pilną įstaigos struktūros sąrašą
Inicijuoti struktūrinio padalinio duomenų pakeitimą	edit(ID)	Struktūrinio padalinio identifikacinis numeris	Struktūrinio padalinio duomenys
Patvirtinti struktūrinio padalinio duomenis	edit(ID, Data)	Struktūrinio padalinio identifikacinis numeris ir kiti užpildyti formos duomenys	Galimas formos klaidų sąrašas ir struktūrinio padalinio duomenys arba atnaujinti struktūrinio padalinio duomenys ir nukreipimas į pilną įstaigos struktūros sąrašą

Ištrinti struktūrinio padalinio duomenis	remove(ID)	Struktūrinio padalinio identifikacinis numeris	Pilnas įstaigos struktūros sąrašas
Peržiūrėti objektų sąrašą	office()		Objektų sąrašas
Inicijuoti naujo objekto duomenų įtraukimą į objektų sąrašą	addOffice()		Objekto duomenys
Patvirtinti naujo objekto duomenų įtraukimą į objektų sąrašą	addOffice(Data)	Užpildyti formos duomenys	Galimas formos klaidų sąrašas ir objekto duomenys arba nukreipimas į objektų sąrašą
Inicijuoti objekto duomenų pakeitimą	editOffice(ID)	Objekto identifikacinis numeris	Objekto duomenys
Patvirtinti pakeistus objekto duomenis	editOffice(ID, Data)	Objekto identifikacinis numeris ir kiti užpildyti formos duomenys	Galimas formos klaidų sąrašas ir objekto duomenys arba atnaujinti objekto duomenys ir nukreipimas į objektų sąrašą
Ištrinti objekto duomenis	removeOffice(ID)	Objekto identifikacinis numeris	Objektų sąrašas

GVSU-4 Užduotis „Vykdysti įstaigų informacinių vertybių skirstymą pagal jų grupes ir rūšis“ pagal GVSR-2 vartotojo sąsają užtikrina DR-4 reikalavimo įgyvendinimą. Šią užduotį sistemos meniu skyriuje „Vertybės“ vykdo vertybių priežiūros grupės nariai siekdamai suskirstyti visas turimas vertybes pagal jų turimus požymius.

5 lentelė. GVSU-4 užduoties aprašas

Veiksmas	Komanda	Parametrai	Duomenys
Peržiūrėti vertybių grupių sąrašą	group()		Vertybių grupių sąrašas
Įtraukti naujają grupę į vertybių grupių sąrašą	addGroup()		Grupės duomenys
Patvirtinti naujos grupės duomenų įtraukimą į vertybių grupių sąrašą	addGroup(Data)	Užpildyti formos duomenys	Galimas formos klaidų sąrašas ir grupės duomenys arba nukreipimas į vertybių grupių sąrašą
Inicijuoti grupės duomenų pakeitimą	editGroup(ID)	Grupės identifikacinis numeris	Grupės duomenys
Patvirtinti pakeistus grupės duomenis	editGroup(ID, Data)	Grupės identifikacinis numeris ir kiti užpildyti formos duomenys	Galimas formos klaidų sąrašas ir grupės duomenys arba atnaujinti grupės duomenys ir nukreipimas į vertybių grupių sąrašą
Ištrinti grupės duomenis	removeGroup(ID)	Grupės identifikacinis numeris	Nukreipimas į vertybių grupių sąrašą
Peržiūrėti vertybių rūsių sąrašą	subgroup()		Vertybių rūsių sąrašas
Inicijuoti naujos rūšies duomenų įtraukimą į vertybių rūsių sąrašą	addSubgroup()		Rūšies duomenys
Patvirtinti naujos rūšies duomenų įtraukimą į	addSubgroup(Data)	Užpildyti formos duomenys	Galimas formos klaidų sąrašas ir rūšies duomenys

vertibių rūšių sąrašą			arba nukreipimas į vertibių rūšių sąrašą
Inicijuoti rūšies duomenų pakeitimą	editSubgroup(ID)	Rūšies identifikacinis numeris	Rūšies duomenys
Patvirtinti pakeistus rūšies duomenis	editSubgroup(ID, Data)	Rūšies identifikacinis numeris ir kiti užpildyti formos duomenys	Galimas formos klaidų sąrašas ir rūšies duomenys arba atnaujinti rūšies duomenys ir nukreipimas į vertibių rūšių sąrašą
Ištrinti rūšies duomenis	removeSubgroup(ID)	Rūšies identifikacinis numeris	Vertibių rūšių sąrašas
Peržiūrėti detalų vertibių sąrašą	listing()		Detalus vertibių sąrašas
Inicijuoti naujos vertybės įtraukimą į detalų vertibių sąrašą	add()		Vertybės duomenys
Patvirtinti naujos vertybės duomenų įtraukimą į detalų vertibių sąrašą	add(Data)	Užpildyti formos duomenys	Galimas formos klaidų sąrašas ir vertybės duomenys arba nukreipimas į vertibių sąrašą
Inicijuoti vertybės duomenų pakeitimą	edit(ID)	Vertybės identifikacinis numeris	Vertybės duomenys
Patvirtinti pakeistus vertybės duomenis	edit(ID, Data)	Vertybės identifikacinis numeris ir kiti užpildyti formos duomenys	Galimas formos klaidų sąrašas ir vertybės duomenys arba atnaujinti vertybės duomenys ir nukreipimas į detalų vertibių sąrašą
Ištrinti vertybės duomenis	remove(ID)	Vertybės identifikacinis numeris	Detalus vertibių sąrašas

GVSRU-5 Užduotis „Vykduti įstaigos inventoriaus priežiūrą“ pagal GVSR-2 vartotojo sasają užtikrina DR-5 reikalavimo įgyvendinimą. Šią užduotį sistemos meniu skyriuje „Inventorius“ vykdo vertibių priežiūros grupės nariai siekdamai užtikrinti jiems priskirtų vertibių sąrašu tinkamą valdymą ir vedamą buhalterinę apskaitą.

6 lentelė. GVSRU-5 užduoties aprašas

Veiksmas	Komanda	Parametrai	Duomenys
Peržiūrėti detalų inventoriaus sąrašą	listing()		Detalus inventoriaus sąrašas
Filtruoti detalų inventoriaus sąrašą	listing(Data)	Užpildyti formos duomenys	Filtruotas inventoriaus sąrašas
Inicijuoti naujo inventoriaus įtraukimą į detalų inventoriaus sąrašą	add()		Inventoriaus duomenys
Patvirtinti naujo inventoriaus duomenų įtraukimą į detalų inventoriaus sąrašą	add(Data)	Užpildyti formos duomenys	Galimas formos klaidų sąrašas ir inventoriaus duomenys arba nukreipimas į inventoriaus sąrašą
Inicijuoti inventoriaus duomenų pakeitimą	manage(ID)	Inventoriaus identifikacinis	Inventoriaus duomenys

		numeris	
Patvirtinti pakeistus inventoriaus duomenis	manage(ID, Data)	Inventoriaus identifikacinis numeris ir kiti užpildyti formos duomenys	Galimas formos klaidų sąrašas ir inventoriaus duomenys arba atnaujinti inventoriaus duomenys ir nukreipimas į inventoriaus sąrašą
Ištrinti inventoriaus duomenis	remove(ID)	Inventoriaus identifikacinis numeris	Inventoriaus sąrašas

GVSU-6 Užduotis „Vykdyti įstaigos vertybės grėsmių ir pažeidžiamumų nustatymą“ pagal GVSR-2 vartotojo sąsają užtikrina DR-6 reikalavimo įgyvendinimą. Šią užduotį sistemos meniu skyriuje „Rizikos valdymas“ vykdo informacijos saugos grupės nariai siekdami apskaitytį baigtinį įstaigos vertybėms kylančių grėsmių ir pažeidžiamumų sąrašą ir nustatyti kurioms vertybėms šios grėsmių/pažeidžiamumų grupės pasireiškia.

7 lentelė. GVSU-6 užduoties aprašas

Veiksmas	Komanda	Parametrai	Duomenys
Peržiūrėti grėsmių šaltinių ir grėsmių sąrašą	threats()		Grėsmių šaltinių ir grėsmių sąrašas
Filtruoti grėsmių sąrašą	threats(Data)	Užpildyti formos duomenys	Grėsmių šaltinių ir filtruotas grėsmių sąrašas
Inicijuoti naujo grėsmių šaltinio įtraukimą į grėsmių šaltinių sąrašą	addThreatGroup()		Grėsmių šaltinio duomenys
Patvirtinti naujo grėsmių šaltinio duomenų įtraukimą į grėsmių šaltinių sąrašą	addThreatGroup(Data)	Užpildyti formos duomenys	Galimas formos klaidų sąrašas ir grėsmių šaltinio duomenys arba nukreipimas į grėsmių šaltinių ir grėsmių sąrašą
Inicijuoti grėsmių šaltinio duomenų pakeitimą	editThreatGroup(ID)	Grėsmių šaltinio identifikacinis numeris	Grėsmių šaltinio duomenys
Patvirtinti pakeistus grėsmių šaltinio duomenis	editThreatGroup(ID, Data)	Grėsmių šaltinio identifikacinis numeris ir kiti užpildyti formos duomenys	Galimas formos klaidų sąrašas ir grėsmių šaltinio duomenys arba atnaujinti grėsmių šaltinio duomenys ir nukreipimas į grėsmių šaltinių ir grėsmių sąrašą
Ištrinti grėsmių šaltinio duomenis	removeThreatGroup(ID)	Grėsmių šaltinio identifikacinis numeris	Grėsmių ir grėsmių šaltinių sąrašas
Inicijuoti naujos grėsmės įtraukimą į grėsmių sąrašą	addThreat()		Grėsmės duomenys
Patvirtinti naujos grėsmės duomenų įtraukimą į grėsmių sąrašą	addThreat(Data)	Užpildyti formos duomenys	Galimas formos klaidų sąrašas ir grėsmės duomenys arba nukreipimas į grėsmių šaltinių ir grėsmių sąrašą

Inicijuoti grėsmės duomenų pakeitimą	editThreat(ID)	Grėsmės identifikacinis numeris	Grėsmės duomenys
Patvirtinti pakeistus grėsmės duomenis	editThreat(ID, Data)	Grėsmės identifikacinis numeris ir kiti užpildyti formos duomenys	Galimas formos klaidų sąrašas ir grėsmės duomenys arba atnaujinti grėsmės duomenys ir nukreipimas į grėsmių šaltinių ir grėsmių sąrašą
Ištrinti grėsmės duomenis	removeThreat(ID)	Grėsmės identifikacinis numeris	Grėsmių sąrašas
Peržiūrėti pažeidžiamumų sąrašą	vulnerabilities()		Pažeidžiamumų sąrašas
Filtruoti pažeidžiamumų sąrašą	vulnerabilities(Data)	Užpildyti formos duomenys	Filtruotas pažeidžiamumų sąrašas
Atnaujinti pažeidžiamumų sąrašo numatytais reikšmės	updateVulnerabilities-Values(IDs, ldef, idef)	Užpildytos grėsmės tikimybės ir poveikio skaitinės vertės	Pažeidžiamumų sąrašas
Inicijuoti naujo pažeidžiamumo įtraukimą į pažeidžiamumų sąrašą	addVulnerabilities()		Pažeidžiamumo duomenys
Patvirtinti naujo pažeidžiamumo duomenų įtraukimą į pažeidžiamumų sąrašą	addVulnerabilities(Data)	Užpildyti formos duomenys	Galimas formos klaidų sąrašas ir pažeidžiamumo duomenys arba nukreipimas į pažeidžiamumų sąrašą
Inicijuoti pažeidžiamumo duomenų pakeitimą	editVulnerabilities(ID)	Pažeidžiamumo identifikacinis numeris	Pažeidžiamumo duomenys
Patvirtinti pakeistus pažeidžiamumo duomenis	editVulnerabilities(ID, Data)	Pažeidžiamumo identifikacinis numeris ir kiti užpildyti formos duomenys	Galimas formos klaidų sąrašas ir pažeidžiamumo duomenys arba atnaujinti pažeidžiamumo duomenys ir nukreipimas į pažeidžiamumų sąrašą
Ištrinti pažeidžiamumo duomenis	removeVulnerability(ID)	Pažeidžiamumo identifikacinis numeris	Pažeidžiamumų sąrašas
Priskirti grėsmės / pažeidžiamumo grupes prie įstaigos disponuojamų vertybų elementų arba įstaigos struktūrinų elementų	attach()		Įstaigos grėsmių / pažeidžiamumų grupių sąrašas
Pasirinkti priskyrimo tipą (pagal įstaigos disponuojamas vertebes arba įstaigos struktūrą) taip pat lygiagrečiai galima filtruoti duomenis pagal grėsmės šaltinius ar grėsmes	attach(Tipas, ID, Data)	Priskyrimo tipas, grėsmės / pažeidžiamumo grupės identifikacinis numeris ir kiti formos duomenys	Įstaigos grėsmių / pažeidžiamumų grupių sąrašas
Ištrinti vieną prie grėsmės / pažeidžiamumo grupės priskirtą vertybęs	removeAttach(ID, Tipas)	Priskyrimo tipas, vertebės ar įstaigos struktūrinio elemento identifikacinis numeris	Įstaigos grėsmių / pažeidžiamumų grupių sąrašas

elementą ar įstaigos struktūrinių elementų			
Ištrinti visus vertybų elementus priskirtus prie vienos grėsmės / pažeidžiamumo grupės	removeAttachItem(ID)	Vertybės elemento identifikacinis numeris	Įstaigos grėsmių / pažeidžiamumų grupių sąrašas
Ištrinti visus įstaigos struktūrinius elementus priskirtus prie vienos grėsmės / pažeidžiamumo grupės	removeAttachPlace(ID)	Įstaigos struktūrinio elemento identifikacinis numeris	Įstaigos grėsmių / pažeidžiamumų grupių sąrašas

GVSRU-7 Užduotis „Vykduti įstaigos vertybų rizikos vertinimo parametru nustatymą“ pagal GVSR-2 vartotojo sąsają užtikrina DR-7 reikalavimo įgyvendinimą. Šią užduotį sistemos meniu skyriuje „Rizikos valdymas“ vykdo informacijos saugos grupės nariai siekdamai grėsmių vizualizavimo prototipą pritaikyti prie įstaigos individualių poreikių vykdant rizikos vertinimą. Šios užduoties metu nustatomi tikimybės, kad pasireikš grėsmės/pažeidžiamumo grupės įvykis, poveikio, kurį sukeltą grėsmės/pažeidžiamumo grupės įvykis, ir rizikos laipsniai.

8 lentelė. GVSRU-7 užduoties aprašas

Veiksmas	Komanda	Parametrai	Duomenys
Peržiūrėti rizikos matricą ir jos komponenčių nustatymus (tikimybė, poveikis ir rizika)	config()		Rizikos matrica ir jos komponenčių duomenys
Keisti rizikos matricos komponenčių nustatymus	config(Data)	Užpildyti formos duomenys	Rizikos matrica ir jos komponenčių duomenys
Inicijuoti naujo nustatymų įrašo sukūrimą	addConfig(Value)	Tikimybė, poveikį ar riziką nusakantis parametras	Tikimybės, poveikio ar rizikos duomenys
Sukurti naują rizikos matricos nustatymų komponentę (tikimybė, poveikis ir rizika)	addConfig(Value, Data)	Tikimybė, poveikį ar riziką nusakantis parametras ir kiti formos duomenys	Rizikos matrica ir jos komponenčių duomenys
Ištrinti pasirinktą rizikos matricos tikimybės komponentės duomenų įrašą	removeThreatConfig(ID)	Tikimybės identifikacinis numeris	Rizikos matrica ir jos komponenčių duomenys
Ištrinti pasirinktą rizikos matricos poveikio komponentės duomenų įrašą	removeVulnerabilityConfig(ID)	Poveikio identifikacinis numeris	Rizikos matrica ir jos komponenčių duomenys
Ištrinti pasirinktą rizikos matricos rizikos komponentės duomenų įrašą	removeRiskConfig(ID)	Rizikos identifikacinis numeris	Rizikos matrica ir jos komponenčių duomenys

GVSU-8 Užduotis „Vykdinti įstaigos vertybių rizikos valdymą ir ataskaitų rengimą“ pagal GVSU-2 vartotojo sąsają užtikrina DR-8 reikalavimo įgyvendinimą. Šią užduotį sistemos meniu skyriuje „Rizikos valdymas“ vykdo informacijos saugos grupės nariai ruošdami rizikos valdymo dokumentaciją.

9 lentelė. GVSU-8 užduoties aprašas

Veiksmas	Komanda	Parametrai	Duomenys
Peržiūrėti atlirkų rizikos valdymo ataskaitų sąrašą	listing()		Rizikos valdymo ataskaitų sąrašas
Pagal naujus duomenis suformuoti naują rizikos valdymo ataskaitą	listing(Data)	Užpildyti formos duomenys	Rizikos valdymo ataskaitų sąrašas
Ištrinti rizikos valdymo ataskaitą	removeAssesment(ID)	Rizikos valdymo ataskaitos identifikacinis numeris	Rizikos valdymo ataskaitų sąrašas
Peržiūrėti rizikos valdymo ataskaitos rizikos vertinimo dalies duomenis	view(ID)	Rizikos valdymo ataskaitos identifikacinis numeris	Rizikos vertinimo sąrašas
Keisti rizikos valdymo ataskaitos rizikos vertinimo dalies duomenis	view(ID, Data)	Rizikos valdymo ataskaitos identifikacinis numeris, skaitinės-žodinės rizikos vertinimo peržiūros parametras ir kiti formos duomenys	Rizikos vertinimo sąrašas
Peržiūrėti rizikos valdymo ataskaitos rizikos tvarkymo dalies duomenis	mitigate(ID)	Rizikos valdymo ataskaitos identifikacinis numeris	Rizikos tvarkymo sąrašas
Keisti rizikos valdymo ataskaitos rizikos tvarkymo dalies duomenis arba atsispausdinti rizikos valdymo ataskaitą	mitigate(ID, Data)	Rizikos valdymo ataskaitos identifikacinis numeris, ataskaitos atsispausdinimo parametrai ir kiti formos duomenys	Rizikos tvarkymo sąrašas

GVSU-9 Užduotis „Vykdinti įstaigos vertybių buvimo vienos vizualizavimą“ pagal GVSU-2 vartotojo sąsają užtikrina DR-9 reikalavimo įgyvendinimą. Šią užduotį sistemos meniu skyriuje „Saugos vizualizacija“ vykdo informacijos saugos grupės nariai siekdami vizualizuoti pasirinktų įstaigos objektų vertybes ir atkreipti dėmesį į joms kylančių grėsmių kritiškumą.

10 lentelė. GVSU-9 užduoties aprašas

Veiksmas	Komanda	Parametrai	Duomenys
-----------------	----------------	-------------------	-----------------

Peržiūrėti įstaigos objektų ir juose vizualizuotų vertybų sąrašą	structure()		Įstaigos objektų ir juose vizualizuotų vertybų sąrašas
Apibrėžti vizualizuojamus objektus ir jų vertybes parenkant vertybėms atitinkamas formas	structure(Data)	Užpildyti formos duomenys	Įstaigos objektų ir juose vizualizuotų vertybų sąrašas
Ištrinti vizualizuoto įstaigos objekto ir jo vertybų duomenis	removeStructure(ID)	Įstaigos objekto identifikacinis numeris	Įstaigos objektų ir juose vizualizuotų vertybų sąrašas
Ištrinti vizualizuoto įstaigos objekto formos duomenis	removeStructureObject(ID)	Įstaigos objekto formos identifikacinis numeris	Įstaigos objektų ir juose vizualizuotų vertybų sąrašas

GVSRU-10 Užduotis „Vykdyti grėsmių vizualizavimą informacijos saugos valdymo procese“ pagal GVSR-2 vartotojo sasają užtikrina DR-10 reikalavimo įgyvendinimą. Šią užduotį sistemos meniu skyriuje „Saugos vizualizacija“ vykdo informacijos saugos grupės nariai.

11 lentelė. GVSRU-10 užduoties aprašas

Veiksmas	Komanda	Parametrai	Duomenys
Peržiūrėti naudojamą rizikos matricą, rizikos valdymo ataskaitą ir vizualizuotų objektų pasirinkimo sąrašus	map()		rizikos matricos, rizikos valdymo ataskaitų ir vizualizuojamų objektų sąrašai
Pasirinkti rizikos valdymo ataskaitą ir vizualizuojamą objektą šio objekto vertybėms kylančių grėsmių vizualizacijai	map(SelectInstitutionOfficeID, SelectRiskAssesmentID)	Vizualizuojamo objekto identifikacinis numeris ir parengtos ataskaitos identifikacinis numeris	rizikos matricos, rizikos valdymo ataskaitų ir vizualizuojamų objektų sąrašai, ir objektui kylančių grėsmių vizualizacija

GVSRU-11 Užduotis „Vykdyti įstaigos vertybėms kylančių grėsmių ir rizikos lygio pokyčių valdymą“ pagal GVSR-2 vartotojo sasają užtikrina DR-11 reikalavimo įgyvendinimą. Šią užduotį sistemos meniu skyriuje „Rizikos valdymas“ vykdo informacijos saugos grupės nariai.

12 lentelė. GVSRU-11 užduoties aprašas

Veiksmas	Komanda	Parametrai	Duomenys
Palyginti rizikos lygių pokyčius laiko ašyje	compare()	Rizikos valdymo ataskaitų identifikaciniai numeriai	vertybėms kylančių grėsmių ir rizikos lygių laiko ašyje pokyčių sąrašas

4.1.1.5. Užduočių formulavimo kalbos reikalavimai

13 lentelėje pateikti GVSU užduotyse naudojamų formavimo kalbos priemonių (langų maketų, piktogramų, meniu juostos) unikalūs numeriai, kurie yra pateikti priede B.

Prisijungus prie sistemos, užduotims formuoti naudojama grafinė vartotojo sasaja GVSU-2, kurioje duomenys kinta tik kintamojoje vartotojo sasajos dalyje. Kiti GVSU-2 elementai yra nekintantys:

UFK-1 viršutinėje dalyje slenkant nuo kairiosios pusės atvaizduojamas VGTU logotipas, slenkant į dešinę pateikiama informacija apie prisijungusį naudotoją, slenkant toliau pateikiama galimybė pasikeisti vartotojo sasajos kalbos nustatymus, o dar toliau yra pateikta nuoroda, kuri skirta atsijungti nuo sistemos.

UFK-2 žemiau UFK-1 atvaizduojama meniu skyrių juosta su eile nuorodų į skyriaus techninius išteklius.

UFK-3 žemiau UFK-2 priklausomai nuo pasirinkto skyriaus atvaizduojama meniu poskyrių juosta su eile nuorodų į atitinkamus skyriaus techninius išteklius.

UFK-4 žemiau UFK-3 atvaizduojamas meniu skyriaus pavadinimas.

UFK-5 žemiau UFK-4 atvaizduojama kintanti vartotojo sasajos dalis, kurios langų maketai ir piktogramos pateikti priede B.

13 lentelė. GVSU užduočių formavimo kalba

<i>Užduoties numeris</i>			
Komanda	Langų maketai	Piktogramos	Meniu
<i>GVSU-1</i>			
login(username, password)	GVSU-1	-	-
<i>GVSU-2</i>			
listUsers()	ULMSR-1	UPR-1, UPR-2, UPR-3	Administratorių skyriaus naudotojų sąrašo poskyris
addUser()	ULMDR-1	UPR-4, UPR-5	Administratorių skyriaus naudotojų sąrašo poskyris
addUser(Data)	ULMDR-1	UPR-4, UPR-5, UPR-6	Administratorių skyriaus naudotojų sąrašo poskyris
editUser(userID)	ULMDR-1	UPR-4, UPR-5	Administratorių skyriaus naudotojų sąrašo poskyris
editUser(userID,Data)	ULMDR-1	UPR-4, UPR-5, UPR-6	Administratorių skyriaus naudotojų sąrašo poskyris
removeUsers(userID)	-	-	Administratorių skyriaus naudotojų sąrašo poskyris
<i>GVSU-3</i>			
institutions()	ULMSR-2	UPR-3	Istaigų skyriaus įstaigų poskyris

institutions(Name)	ULMSR-2	UPR-3	Įstaigų skyriaus įstaigų poskyris
removeInstitution(ID)	-	-	Įstaigų skyriaus įstaigų poskyris
listing()	ULMSR-1	UPR-7, UPR-8, UPR-9	Įstaigų skyriaus struktūrinį padalinių poskyris
add()	ULMDR-1	-	Įstaigų skyriaus struktūrinį padalinių poskyris
add(Data)	ULMDR-1	UPR-6	Įstaigų skyriaus struktūrinį padalinių poskyris
edit(ID)	ULMDR-1	-	Įstaigų skyriaus struktūrinį padalinių poskyris
edit(ID, Data)	ULMDR-1	UPR-6	Įstaigų skyriaus struktūrinį padalinių poskyris
remove(ID)	-	-	Įstaigų skyriaus struktūrinį padalinių poskyris
office()	ULMSR-1	UPR-2	Įstaigų skyriaus objektų poskyris
addOffice()	ULMDR-1		Įstaigų skyriaus objektų poskyris
addOffice(Data)	ULMDR-1	UPR-6	Įstaigų skyriaus objektų poskyris
editOffice(ID)	ULMDR-1		Įstaigų skyriaus objektų poskyris
editOffice(ID, Data)	ULMDR-1	UPR-6	Įstaigų skyriaus objektų poskyris
removeOffice(ID)	-	-	Įstaigų skyriaus objektų poskyris

GVSU-4

group()	ULMSR-1	UPR-2, UPR-8, UPR-9	Vertybų skyriaus vertybių grupės poskyris
addGroup()	ULMDR-1	-	Vertybų skyriaus vertybių grupės poskyris
addGroup(Data)	ULMDR-1	UPR-6	Vertybų skyriaus vertybių grupės poskyris
editGroup(ID)	ULMDR-1	-	Vertybų skyriaus vertybių grupės poskyris
editGroup(ID, Data)	ULMDR-1	UPR-6	Vertybų skyriaus vertybių grupės poskyris
removeGroup(ID)	-	-	Vertybų skyriaus vertybių grupės poskyris
subgroup()	ULMSR-1	UPR-2, UPR-8, UPR-9	Vertybų skyriaus vertybių rūšies poskyris
addSubgroup()	ULMDR-1	-	Vertybų skyriaus vertybių rūšies poskyris
addSubgroup(Data)	ULMDR-1	UPR-6	Vertybų skyriaus vertybių rūšies poskyris
editSubgroup(ID)	ULMDR-1	-	Vertybų skyriaus vertybių rūšies poskyris
editSubgroup(ID, Data)	ULMDR-1	UPR-6	Vertybų skyriaus vertybių rūšies poskyris
removeSubgroup(ID)	-	-	Vertybų skyriaus vertybių rūšies poskyris
listing()	ULMSR-1	UPR-2, UPR-8, UPR-9	Vertybų skyriaus vertybių poskyris

add()	ULMDR-1	-	Vertybų skyriaus vertybių poskyris
add(Data)	ULMDR-1	UPR-6	Vertybų skyriaus vertybių poskyris
edit(ID)	ULMDR-1	-	Vertybų skyriaus vertybių poskyris
edit(ID, Data)	ULMDR-1	UPR-6	Vertybų skyriaus vertybių poskyris
remove(ID)	-	-	Vertybų skyriaus vertybių poskyris
<i>GVSRU-5</i>			
listing()	ULMSR-3	UPR-2, UPR-3, UPR-7, UPR-10, UPR-12	Inventoriaus skyriaus inventoriaus poskyris
listing(Data)	ULMSR-3	UPR-2, UPR-3, UPR-7, UPR-10, UPR-11, UPR-12	Inventoriaus skyriaus inventoriaus poskyris
add()	ULMDR-1	UPR-11	Inventoriaus skyriaus inventoriaus poskyris
add(Data)	ULMDR-1	UPR-6, UPR-11	Inventoriaus skyriaus inventoriaus poskyris
manage(ID)	ULMDR-1	UPR-11	Inventoriaus skyriaus inventoriaus poskyris
manage(ID, Data)	ULMDR-1	UPR-6, UPR-11	Inventoriaus skyriaus inventoriaus poskyris
remove(ID)	-	-	Inventoriaus skyriaus inventoriaus poskyris
<i>GVSRU-6</i>			
threats()	ULMSR-4	UPR-1, UPR-2	Rizikos valdymo skyriaus Grėsmių sąrašo poskyris
threats(Data)	ULMSR-4	UPR-1, UPR-2	Rizikos valdymo skyriaus Grėsmių sąrašo poskyris
addThreatGroup()	ULMDR-1	-	Rizikos valdymo skyriaus Grėsmių sąrašo poskyris
addThreatGroup(Data)	ULMDR-1	UPR-6	Rizikos valdymo skyriaus Grėsmių sąrašo poskyris
editThreatGroup(ID)	ULMDR-1		Rizikos valdymo skyriaus Grėsmių sąrašo poskyris
editThreatGroup(ID, Data)	ULMDR-1	UPR-6	Rizikos valdymo skyriaus Grėsmių sąrašo poskyris
removeThreatGroup(ID)	-	-	Rizikos valdymo skyriaus Grėsmių sąrašo poskyris
addThreat()	ULMDR-1	-	Rizikos valdymo skyriaus Grėsmių sąrašo poskyris
addThreat(Data)	ULMDR-1	UPR-6	Rizikos valdymo skyriaus Grėsmių sąrašo poskyris
editThreat(ID)	ULMDR-1		Rizikos valdymo skyriaus Grėsmių sąrašo poskyris
editThreat(ID, Data)	ULMDR-1	UPR-6	Rizikos valdymo skyriaus Grėsmių sąrašo poskyris
removeThreat(ID)	-	-	Rizikos valdymo skyriaus Grėsmių sąrašo poskyris
vulnerabilities()	ULMSR-5	UPR-2	Rizikos valdymo skyriaus Pažeidžiamumų sąrašo poskyris
vulnerabilities(Data)	ULMSR-5	UPR-2	Rizikos valdymo skyriaus Pažeidžiamumų sąrašo

			poskyris
addVulnerabilities()	ULMDR-1	-	Rizikos valdymo skyriaus Pažeidžiamumų sąrašo poskyris
addVulnerabilities(Data)	ULMDR-1	UPR-6	Rizikos valdymo skyriaus Pažeidžiamumų sąrašo poskyris
editVulnerabilities(ID)	ULMDR-1	-	Rizikos valdymo skyriaus Pažeidžiamumų sąrašo poskyris
editVulnerabilities(ID, Data)	ULMDR-1	UPR-6	Rizikos valdymo skyriaus Pažeidžiamumų sąrašo poskyris
removeVulnerability(ID)	-	-	Rizikos valdymo skyriaus Pažeidžiamumų sąrašo poskyris
attach()	ULMSR-6	UPR-3	Rizikos valdymo Priskyrimo poskyris
attach(Tipas, ID, Data)	ULMSR-6	UPR-3	Rizikos valdymo Priskyrimo poskyris
removeAttach(ID, Tipas)	-	-	Rizikos valdymo Priskyrimo poskyris
removeAttachItem(ID)	-	-	Rizikos valdymo Priskyrimo poskyris
removeAttachPlace(ID)	-	-	Rizikos valdymo Priskyrimo poskyris

GVSRU-7

config()	ULMSR-7	UPR-3, UPR-7	Rizikos valdymo Nustatymų poskyris
config(Data)	ULMSR-7	UPR-3, UPR-7	Rizikos valdymo Nustatymų poskyris
addConfig(Value, Data)	ULMDR-1	UPR-6	Rizikos valdymo Nustatymų poskyris
removeThreatConfig(ID)	-	-	Rizikos valdymo Nustatymų poskyris
removeVulnerabilityConfig(ID)	-	-	Rizikos valdymo Nustatymų poskyris
removeRiskConfig(ID)	-	-	Rizikos valdymo Nustatymų poskyris

GVSRU-8

listing()	ULMSR-8	UPR-3	Rizikos valdymo Rizikos valdymo poskyris
listing(Data)	ULMSR-8	UPR-3, UPR-6	Rizikos valdymo Rizikos valdymo poskyris
removeAssesment(ID)	-	-	Rizikos valdymo Rizikos valdymo poskyris
view()	ULMSR-9	-	Rizikos valdymo Rizikos valdymo poskyris
view(Data)	ULMSR-9	-	Rizikos valdymo Rizikos valdymo poskyris
mitigate()	ULMSR-9	-	Rizikos valdymo Rizikos valdymo poskyris
mitigate(Data)	ULMSR-9	-	Rizikos valdymo Rizikos valdymo poskyris

GVSRU-9

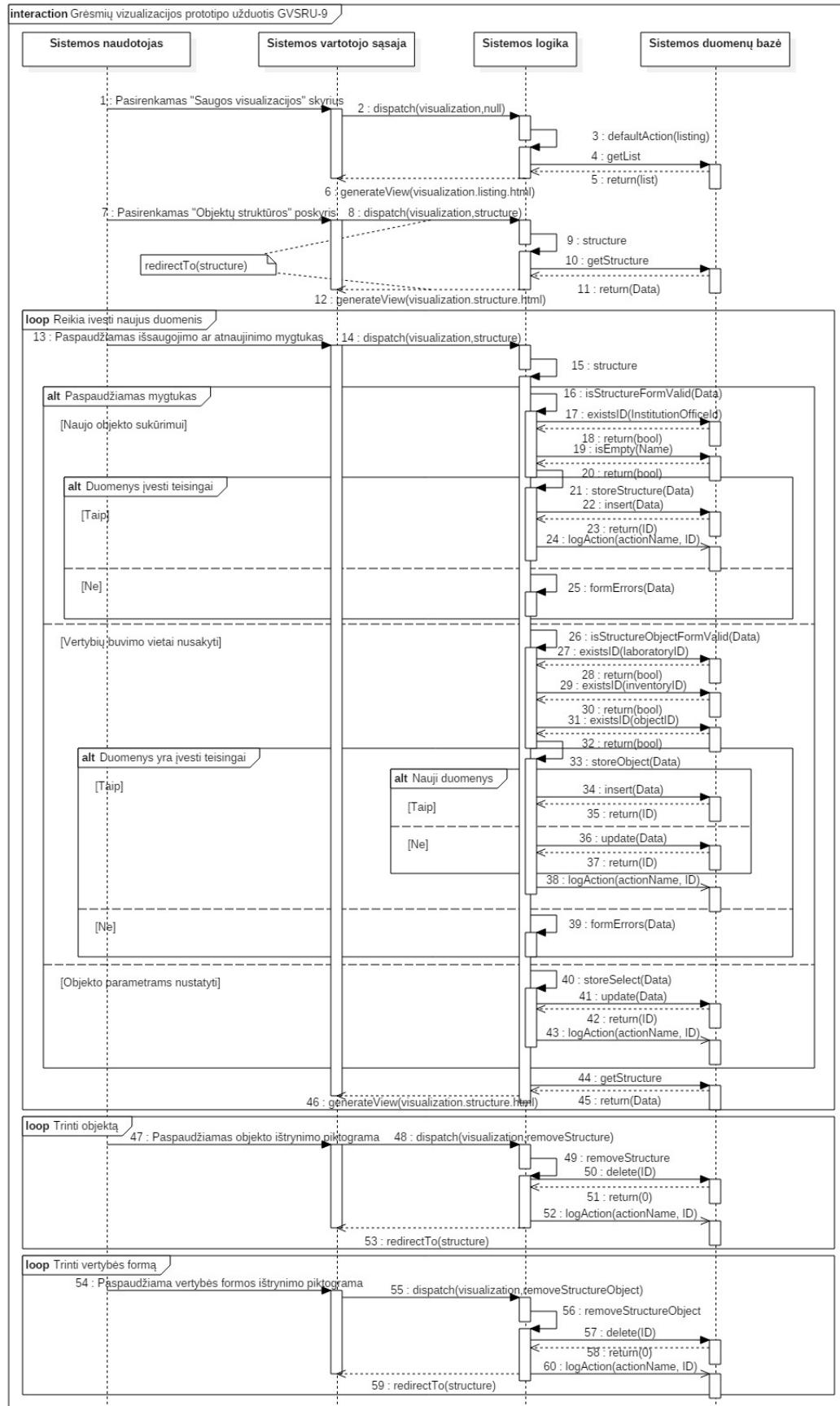
structure()	ULMSR-10	UPR-3, UPR-13	Saugos vizualizacijos skyriaus Objektų vizualizacijos poskyris
structure(Data)	ULMSR-10	UPR-3, UPR-6, UPR-13	Saugos vizualizacijos skyriaus Objektų vizualizacijos poskyris
removeStructure(ID)	-	-	Saugos vizualizacijos skyriaus Objektų vizualizacijos poskyris
removeStructureObject(I D)	-	-	Saugos vizualizacijos skyriaus Objektų vizualizacijos poskyris
<i>GVSRU-10</i>			
map()	ULMSR-11	-	Saugos vizualizacijos skyriaus Rizikos vizualizavimo poskyris
map(SelectInstitutionOf- ficeID, SelectRiskAssesmentID)	ULMSR-11	UPR-6	Saugos vizualizacijos skyriaus Rizikos vizualizavimo poskyris
<i>GVSRU-11</i>			
compare()	ULMSR-12	UPR-14, UPR-15, UPR-16, UPR-17, UPR-18, UPR-19, UPR-20, UPR-21	Rizikos valdymo skyriaus Rizikos valdymo poskyris

4.1.1.6. Užduočių formulavimo būdo (protokolo) reikalavimai

Užduočių formulavimo būdo reikalavimuose (UFBR) bus nagrinėjami tik dalykiniuose reikalavimuose (DR) apibrėžtos užduotys, pagalbinės sistemos funkcijos yra nenagrinėjamos.

Užduočių formulavimo būdo reikalavimai, kurie nėra šio magistro tezių objektas yra iškelti į priedą C.

UFBR-9 Pagal GVSR-2 vartotojo sąsają užduoties GVSRU-9 vykdymo žingsniai atvaizduoti UML sekų diagramoje (žr. 11 pav.). Kaip ir UFBR-1 šioje sekų diagramoje pateikti ryšiai tarp tų pačių sistemos 4 elementų nenagrinėjant GVSR-1 vartotojo sąsajos dalies.



11 pav. GVSU-9 užduoties sekų diagrama

Sekų diagramoje (žr. 11 pav.) pateikti sistemos elementų tarpusavio sąveikos žingsniai, kuriuos vykdo informacijos saugumo grupės narys siekdamas apibrėžti analizuojamo objekto struktūrą ir disponuojamų vertybių būvimo vietą šiame objekte:

1–6 informacijos saugumo grupės nariui pasirinkus meniu skyrių „Saugos vizualizacija“ sistema komanda *listing* pateikia vertybių vizualizacijos formų sąrašą;

7–12 informacijos saugumo grupės nariui pasirinkus „Saugos vizualizacija“ meniu skyriaus „Objektų struktūra“ poskyrį sistema pateikia vizualizuotų įstaigos objektų sąrašą pagal GVSRU-9 *structure* komanda suformuotą ULMSR-10 langą;

13–15 informacijos saugumo grupės narys siekdamas sukurti naują objektą ULMSR-10 lange pasirenka įstaigos, padalinio ir objekto reikšmes ir įveda jas apibūdinantį pavadinimą, ir naujo objekto sukūrimo formoje spaudžia mygtuką „Išsaugoti“. Sistema vykdo komandą *structure*;

16–20 sistema vykdo naujo objekto sukūrimo formos duomenų patikrinimą;

21–24 jeigu duomenys yra įvesti taisyklingai (tinkamos objekto identifikacinis numeris, objektą apibūdinančio pavadinimo laukas nėra paliktas tuščias), tada vykdomas šių duomenų išsaugojimas duomenų bazėje, taip pat išsaugojama atlikto veiksmo žyma;

25 jeigu duomenys yra įvesti netaisyklingai sistema formuoja klaidos pranešimą;

44–46 sistema pateikia vizualizuotų įstaigos objektų sąrašą pagal GVSRU-9 *structure* komanda suformuotą ULMSR-10 langą;

13–15 informacijos saugumo grupės narys siekdamas nustatyti vertybių būvimo vietą objekte ULMSR-10 lange įveda arba pakeičia vertybės ir jos formos duomenis ir puslapiaivimo nustatymą ir mygtukų juosteje spaudžia mygtuką „Atnaujinti“. Sistema vykdo komandą *structure*;

26–32 sistema vykdo vertybės ir jos formos duomenų patikrinimą;

33–38 jeigu duomenys yra įvesti taisyklingai (tinkamai parinkti identifikacinių duomenys), tada vykdomas naujų duomenų išsaugojimas arba senų duomenų atnaujinimas duomenų bazėje, taip pat išsaugojama atlikto veiksmo žyma;

39 jeigu duomenys yra įvesti netaisyklingai sistema formuoja klaidos pranešimą;

44–46 sistema pateikia atnaujintus vertybės ir jos formos duomenis pagal GVSRU-9 *structure* komanda suformuotą ULMSR-10 langą. Priklasomai nuo įvestų duomenų objekto vertybių vizualizacijoje pasislenka vertybės forma;

13–15 informacijos saugumo grupės narys siekdamas nustatyti objekto parametrus ULMSR-10 lange pakeičia objekto parametru duomenis ir objekto pasirinkimo ir matmenų nustatymo formoje spaudžia mygtuką „Atnaujinti“. Sistema vykdo komandą *structure*;

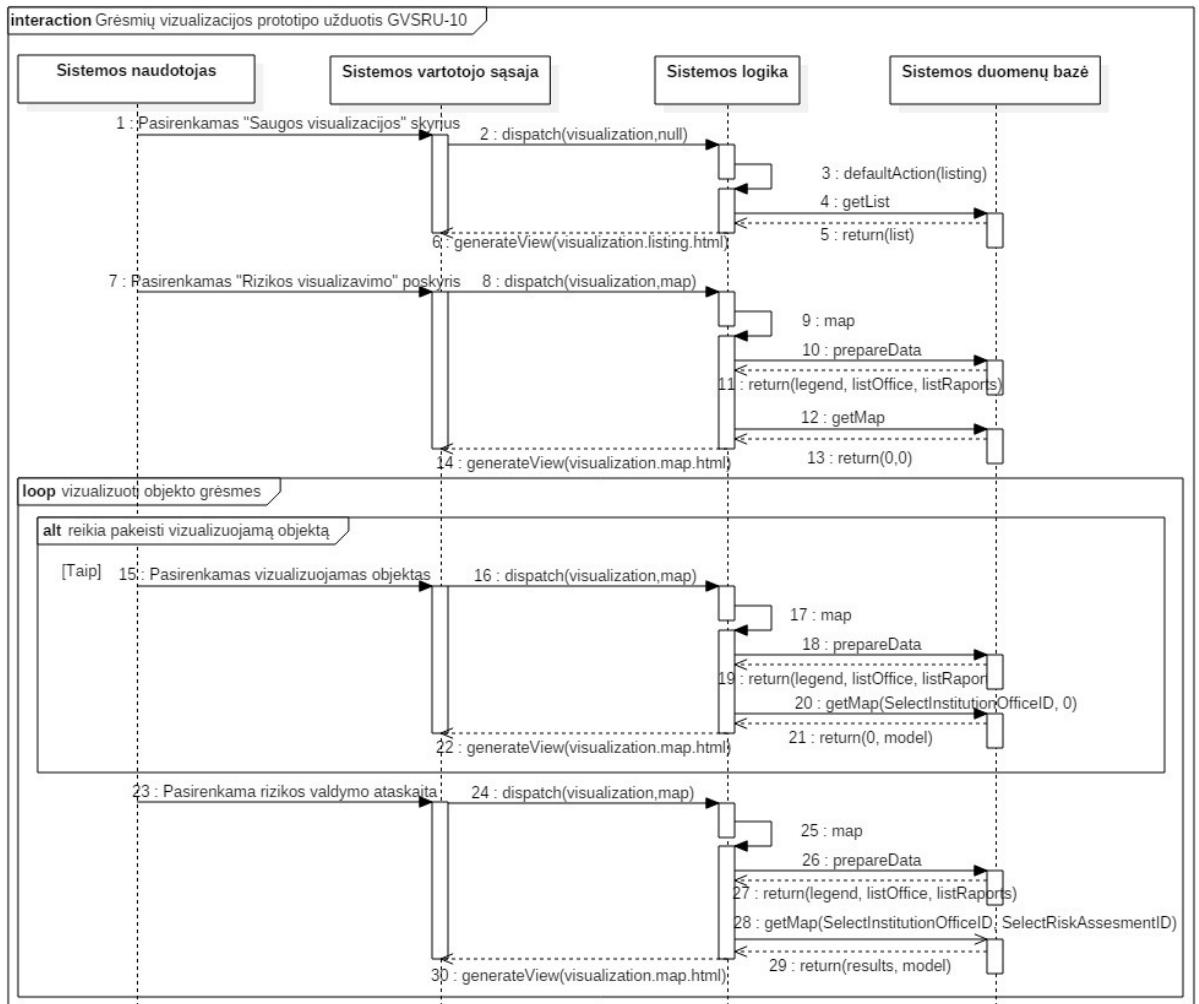
40–43 vykdomas objekto parametru atnaujinimas duomenų bazėje, taip pat išsaugojama atlikto veiksmo žyma;

44–46 sistema pateikia naujas objekto matmenis pagal GVSRU-9 *structure* komanda suformuotą ULMSR-10 langą. Priklausomai nuo įvestų duomenų objekto vertybų vizualizacijoje pasikeičia objekto ilgis ir plotis;

47–53 informacijos saugumo grupės narys siekiantis ištinti neberekalingą objektą spaudžia ULMSR-10 lange pateiktame objekto duomenų juostoje esančią UPR-3 piktogramą. Sistema įvykdo komandą *removeStructure* ir iština pasirinktą objektą, išsaugoja atlikto veiksmo žymą ir informacijos saugumo grupės narys nukreipiamas į vizualizuotų įstaigos objektų sąrašą (8–12 žingsniai).

54–59 informacijos saugumo grupės narys siekiantis ištinti neberekalingą vertybės formą objekte spaudžia ULMSR-10 lange pateiktame vertybės ir jos formos duomenų juostoje esančią UPR-13 piktogramą. Sistema įvykdo komandą *removeStructureObject* ir iština pasirinktą vertybės formą, išsaugoja atlikto veiksmo žymą ir informacijos saugumo grupės narys nukreipiamas į vizualizuotų įstaigos objektų sąrašą (8–12 žingsniai).

UFBR-10 Pagal GVSR-2 vartotojo sąsają užduoties GVSRU-10 vykdymo žingsniai atvaizduoti UML sekų diagramoje (žr. 12 pav.). Kaip ir UFBR-1 šioje sekų diagramoje pateikti ryšiai tarp tų pačių sistemos 4 elementų nenagrinėjant GVSR-1 vartotojo sąsajos dalies.



12 pav. GVSU-10 užduoties sekų diagrama

Sekų diagramoje (žr. 12 pav.) pateikti sistemos elementų tarpusavio sąveikos žingsniai, kuriuos vykdo informacijos saugumo grupės narys siekdamas vizualizuoti objekto vertybėms kylančias grėsmes ir riziką:

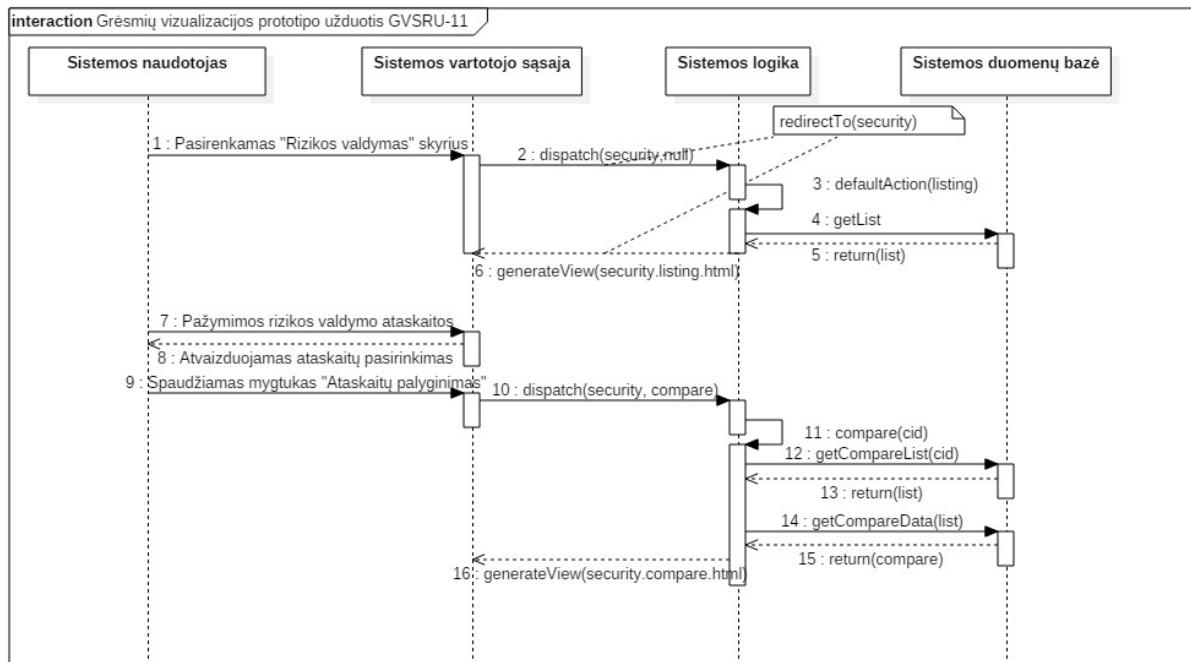
1–6 informacijos saugumo grupės nariui pasirinkus meniu skyrių „Saugos vizualizacija“ sistema komanda *listing* pateikia vertybų vizualizacijos formų sąrašą;

7–14 informacijos saugumo grupės nariui pasirinkus „Saugos vizualizacija“ meniu skyriaus „Rizikos vizualizavimas“ poskyrių sistema pateikia rizikos valdymo ataskaitų vizualizavimo įrankį pagal GVSU-10 *map* komanda suformuotą ULMSR-11 langą;

15–22 informacijos saugumo grupės narys siekdamas vizualizuoti objektą pagal turimą rizikos valdymo ataskaitą pirmiausiai turi pasirinkti „Objektų struktūros“ poskyryje vizualizuotą objektą. Po šio pasirinkimo sistema vykdo GVSU-10 *map* komandą ir atvaizduoja pasirinkto objekto vertybų vizualizaciją;

23–30 informacijos saugumo grupės narys pasirenka rizikos valdymo ataskaitą, vykdoma GVSRU-10 *map* komanda ir ULMSR-11 lange atvaizduojama pasirinktame objekte kylančių grėsmių ir rizikos vizualizacija. Taip pat atvaizduojamas objektui kylančių grėsmių ir rizikų sąrašas bei skaičiavimo duomenys.

UFBR-11 Pagal GVSR-2 vartotojo sąsają užduoties GVSRU-11 vykdymo žingsniai atvaizduoti UML sekų diagramoje (žr. 13 pav.). Kaip ir UFBR-1 šioje sekų diagramoje pateikti ryšiai tarp tų pačių sistemos 4 elementų nenagrinėjant GVSR-1 vartotojo sąsajos dalies.



13 pav. GVSRU-11 užduoties sekų diagramos dalis

Sekų diagramoje (žr. 13 pav.) pateikti sistemos elementų tarpusavio sąveikos žingsniai, kuriuos vykdo informacijos saugumo grupės narys siekdamas analizuoti įstaigos vertybėms kylančių grėsmių ir rizikos pokyčius:

1–6 informacijos saugumo grupės nariui pasirinkus meniu skyrių „Rizikos valdymas“ sistema pateikia rizikos valdymo ataskaitų sąrašą pagal GVSRU-11 *listing* komanda suformuotą ULMSR-8 langą;

7–8 informacijos saugumo grupės narys sužymi visas rizikos valdymo ataskaitas, kurių rizikos pokyčius siekiama analizuoti;

9–16 informacijos saugumo grupės nariui spaudus mygtuką „Ataskaitų palyginimas“ sistema pateikia įstaigos vertybėms kylančių grėsmių ir rizikų pokyčių duomenis laiko ašyje pagal GVSRU-11 *compare* komanda suformuotą ULMSR-12 langą.

4.1.1.7. Sąsajos darnos ir standartizavimo reikalavimai

IDSR-1 Sistema turi turėti grafinę vartotojo sąsają, kurios elementų pozicija, meniu, naudojamos spalvos, piktogramos ir dialogo langai būtų tarpusavyje suderinti ir atvaizduojami standartinėse vartotojo sąsajos vietose neklaidinant sistemos naudotojų.

IDSR-2 Sistemos piktogramos, mygtukai ir teksto nuorodos turi atlikti tik tas funkcijas, kurioms jos yra skirtos, kad nebūtų klaidinami sistemos naudotojai.

IDSR-3 Sistemos vartotojo sąsajos turi būti kuriami pagal HTML 5 standartą.

4.1.1.8. Pranešimų formulavimo reikalavimai

PFR-1 Sistema turi formuoti informacinius pranešimus ant grafinių sistemos elementų, kuriuose būtų pateiktas grafinio elemento paskirties pranešimas.

PFR-2 Sistema turi formuoti klaidų pranešimus, jeigu sistemos naudotojas atlieka draudžiamus veiksmus arba neteisingai atlieka duomenų įvedimo ar pakeitimo veiksmus.

PFR-3 Visi pranešimai turi būti vaizduojami pagal sistemos naudotojo pasirinktą kalbą.

4.1.1.9. Sąsajos individualizavimo reikalavimai

IIR-1 Sistema turi leisti sistemos naudotojams galimybę pasikeisti vartotojo sąsajos kalbą: iš lietuvių į anglų ir iš anglų į lietuvių kalbą.

4.1.2. Funkciniai reikalavimai

4.1.2.1. Dalykiniai reikalavimai

DR-1 Sistema turi leisti administratoriui ir jos naudotojams identifikuotis su savo asmeniniu vartotojo vardu ir slaptažodžiu.

Sistemos administratoriui:

DR-2 Sistema turi leisti kurti sistemos naudotojus ir jiems priskirti atitinkamus vaidmenis.

Vertybų priežiūros grupei:

DR-3 Sistema turi leisti kurti įstaigų, jos struktūrinių padalinių, objektų sąrašus.

DR-4 Sistema turi leisti kurti vertybų grupių, rūsių, pavadinimų sąrašus.

DR-5 Sistema turi leisti kurti įstaigose disponuojamo inventorius sąrašus.

Informacijos saugumo grupei:

DR-6 Sistema turi leisti kurti įvairiomis proporcijomis grėsmių šaltinių, grėsmių, pažeidžiamumų sąrašus ir priskirti grėsmių/pažeidžiamumų grupes prie vertybų ar jų būvimo vienos.

DR-7 Sistema turi leisti nevaržomai keisti rizikos matricą keičiant jos komponenčių (tikimybės, poveikio ir rizikos) nustatymus.

DR-8 Sistema turi leisti vertinti ir tvarkyti įstaigos vertybėms kylančią riziką ir pareikalavus automatiškai suformuoti rizikos valdymo ataskaitas PDF ar XLS formatu.

DR-9 Sistema turi leisti apibrėžti įstaigos vertybų būvimo vietą objektuose (nustatyti geolokaciją).

DR-10 Sistema turi leisti iš rizikos vertinimo ataskaitos ir objekto, kuriamo yra apibrėžtos vertybės, duomenų, vizualizuoti tame objekte esančias vertybes pagal pasireiškiančių grėsmių kritiškumą.

DR-11 Sistema turi leisti laiko ašyje stebėti kaip kinta įstaigos vertybėms kylančių grėsmių ir rizikų kritiškumas.

4.1.2.2. Pagalbinės sistemos funkcijos

PSR-1 Sistema turi leisti kurti vartotojų sąsajų šablonus ir nustatyti prieigos parametrus prie techninių sistemos išteklių.

PSR-2 Sistema turi kaupti kiekvieno sistemos naudotojo atlanko veiksmo žurnalinius įrašus.

PSR-3 Sistema turi kaupti kiekvieno inventoriaus duomenų pakeitimo žurnalinius įrašus.

PSR-4 Sistema turi leisti komentuoti įstaigos inventoriaus įvykius ir pakeisti vertybės būseną.

PSR-5 Sistema turi leisti apibrėžti inventoriaus vidines savybes.

PSR-6 Sistemoje turi būti realizuota patogi inventoriaus paieška pagal vertybės duomenis.

PSR-7 Sistema turi leisti filtruoti duomenis pagal šių duomenų esminius bruožus.

PSR-8 Sistema turi leisti keisti vartotojo sąsajos kalbos nustatymus.

PSR-9 Sistema turi leisti peržiūrėti įdiegtas sistemoje kiekvienos vertybės vizualizaciją.

PSR-10 Sistema turi leisti formuoti ir išsaugoti grėsmių vizualizacijas PNG formatu.

PSR-11 Sistema turi leisti išsaugotas grėsmių vizualizacijas pridėti prie vizualizuojamos rizikos valdymo ataskaitos.

4.1.3. Nefunkciniai reikalavimai

4.1.3.1. Vidiniai sąsajos reikalavimai

4.1.3.2. Operacinės sistemos naudojimo reikalavimai

OSNR-1 Sistema gali veikti bet kurioje operacinėje sistemoje, kurioje veiktu „PHP“ programavimo kalba, „Apache“ interneto serveris ir „MySQL“ ar „PostgreSQL“ duomenų bazė.

OSNR-2 Sistemos naudotojai atliekantys sistemos administravimą gali dirbti bet kurioje operacinėje sistemoje, kurioje būtų įdiegta interneto naršyklė.

4.1.3.3. Sąveikos su duomenų bazėmis reikalavimai

DBR-1 Sistema gali naudoti „MySQL“ arba „PostgreSQL“ reliacinių duomenų bazų valdymo sistemą.

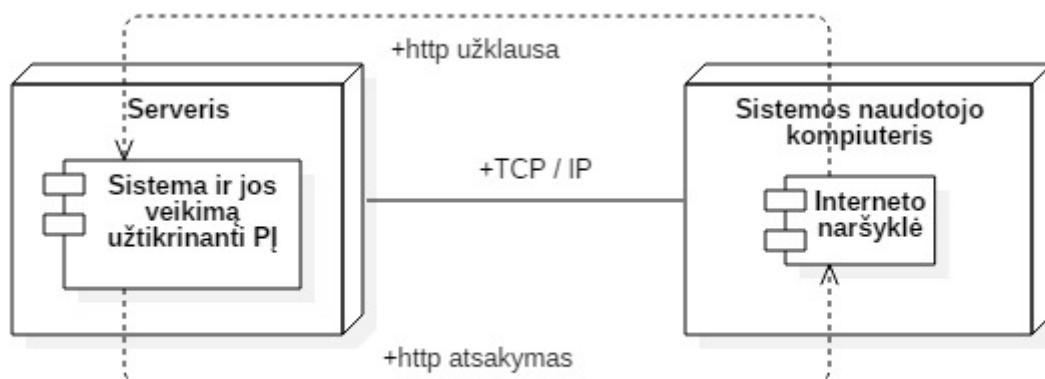
4.1.3.4. Dokumentų mainų reikalavimai

DMR-1 Rizikos valdymo ataskaitos formuojamos PDF arba XLS formatu ir gali būti išsaugojamos sistemos naudotojo kompiuteryje.

DMR-2 Grėsmių vizualizacijos serveryje išsaugojamos PNG formatu pagal sistemos naudotojo sistemoje matomą vizualizacijos atvaizdą.

4.1.3.5. Darbo kompiuterių tinkluose reikalavimai

Sistemos veikimo užtikrinimui serveris turi būti ekspluatuojamas pagal OSNR-1 reikalavimą. Prie sistemos naudotojai jungiasi su kompiuteriu ar kitu įrenginiu, kurio operacinėje sistemoje yra įdiegta interneto naršyklė palaikanti WebGL naudojantis http(s) protokolu, tai galima iliustruoti komponentų diagrama (žr. 14 pav.).



14 pav. Komponentų pasiskirstymas kompiuterių tinkle schema

DKTR-1 Sistemos naudotojai turi pasiekti serverį, kuriame funkcionuoja sistema, naudojant interneto naršyklę.

DKTR-2 Darbui tinkle turi būti naudojamas TCP/IP protokolas.

DKTR-3 Tarp sistemos naudotojo ir serverio turi vykti užklausimai – atsakymai HTTP protokolu.

DKTR-4 Interneto serveris turi suteikti pakankamą pralaidumą ir galimų prisijungimų kiekj, kad būtų tinkamai aptarnaujamas sistemos naudotojas.

4.1.3.6. Sąveikos su kitomis programomis reikalavimai

SKPR-1 Sistemos naudotojo interneto naršyklė turi palaikyti WebGL funkcionalumą.

4.1.3.7. Programavimo aplinkos reikalavimai

PAR-1 Sistemos serverio dalis programuojama PHP kalba.

PAR-2 Sistemos programavimui naudoti ne mažesnį nei PSR-1 pagrindinį kodavimo standartą.

PAR-3 Sistemos klientinė dalis koduojama JavaScript kalba, žymima HTML ir CSS kalba.

4.1.3.8. Veikimo reikalavimai

4.1.3.9. Tikslumo reikalavimai

Vaizdavimo tikslumo reikalavimai:

VTR-1 Sistemos naudotojų veiksmai vaizduojami sekundės tikslumu.

VTR-2 Inventoriaus kiekis vaizduojamas vienetų tikslumu.

VTR-3 Rizikos matricos komponentės (tikimybė, poveikis ir rizika) vaizduojama vieno skaitmens po kablelio tikslumu.

VTR-4 Rizikos matricos komponenčių reikšmes ir jų klasifikaciją individualiai nusistato kiekvienas įstaigos sistemos naudotojas.

VTR-5 Rizikos valdymo ataskaitos vaizduojamos dienos tikslumu.

VTR-6 Verybės objekte vaizduojamos trimatėje Dekarto koordinačių ašyje vienetų tikslumu ir sukamos aplink koordinačių ašis laipsnio tikslumu.

VTR-7 Grėsmės vizualizuojamos pagal sistemos naudotojo nustatytas spalvas, kurias palaiko visos šiuolaikinės interneto naršyklės [37].

VTR-8 Objekto matmenys vaizduojami centimetru tikslumu.

Skaičiavimų tikslumo reikalavimai:

STR-1 Sistemos naudotojų veiksmų žurnaliniai įrašai saugomi sekundės tikslumu.

STR-2 Inventoriaus kiekis skaičiuojamas vieneto tikslumu.

STR-3 Rizikos matricos komponentės (tikimybės, poveikio ir rizikos) nustatymai skaičiuojami vieno skaitmens po kablelio tikslumu.

STR-4 Rizika vertinama vieno skaitmens po kablelio tikslumu.

STR-5 Vertybės objekte dydžiai nustatomi vieneto tikslumu.

STR-6 Objekto matmenys nustatomi vieneto tikslumu.

4.1.3.10. Patikimumo reikalavimai

PR-1 Sistemos patikimumui užtikrinti tinklas ir serveris, kuriami jis yra eksplotuojamas, turi būti tinkamai sukonfigūruotas, kad būtų galima išvengti kuo daugiau darbo trikių ir patvirtintos atitinkamos procedūros.

PR-2 Sistemos naudotojui išsaugant duomenis sistemoje, kurie neatitinka jos reikalavimų, turi būti siunčiamas klaidos ar įvykio pranešimas taip išvengiant duomenų sugadinimo galimybės.

PR-3 Sistemos serveris turi būti laikomas tinkamos temperatūros vėdinamoje aplinkoje ir apsaugotas nepertraukiamais maitinimo šaltiniais.

PR-4 Istaigoje turi būti vykdomi sistemos aparatinės įrangos periodiniai atnaujinimo darbai.

PR-5 rekomenduojama turėti atsarginę sistemos aplinką, kurioje testavimo tikslais pirmiausiai būtų vykdomas sistemos funkcionalumo keitimas, programinės įrangos atnaujinimai ar kiti veiksmai, kurie potencialiai galėtų sutrikdyti sistemos darbą.

4.1.3.11. Robastiškumo reikalavimai

RR-1 Istaigoje sistemos serverio operacinės sistemos priemonėmis turi būti automatizuotai vykdomas sistemos atsarginių duomenų kopijų iniciavimas ir išsaugojimas serveryje ar nutolusiame atsarginių kopijų serveryje ir patvirtintos atitinkamos procedūros.

RR-2 Istaigoje turi būti nustatytas periodiškumas kaip dažnai yra vykdomos atsarginės sistemos kopijos.

RR-3 Įstaigoje turi būti vykdomi bandymai siekiant atstatyti serverio funkcionalumą ir sistemos funkcionalumą vykdant atstatymo iš atsarginių kopijų bandymus, taip pat turi būti patvirtintos šių darbų atitinkamos procedūros.

4.1.3.12. Našumo reikalavimai

3D turinio pristatymas tinkle yra užvėlinamas atsižvelgiant į siunčiamas medijos rinkmenas tokias kaip tekstas, nejudančios nuotraukos, vaizdo ir garso įrašai [38]. Grėsmių vizualizavimo prototipo sistemoje tinklu bus persiunčiami vertybų formos rinkmenos OBJ formatu, kuriame yra saugojamas vertybės formos kodas ir kita su persiunčiama forma susijusi informacija, o taip pat su OBJ formato rinkmena gali būti siunčiama ir MTL formato rinkmena, kuri apvilkę vertybės formą atitinkama medžiaga, pavyzdžiu pateikiama nuotraukos pavidalu JPG formatu ar kita. OBJ formato rinkmenos gali būti nuo dešimčių kilobaitų iki kelių ar daugiau megabaitų, todėl dėl didelio kieko vertybų atvaizdavimo gali kilti sistemos našumo problemų. Sistemos valdytojo siekiamybė našumui gerinti būtų mažesnių OBJ rinkmenų naudojimas, spartesnis tinklo pralaidumas ir našesnė sistemos naudotojų kompiuterinė įranga, kuri leistų greičiau apdoroti 3D vizualizaciją.

NAR-1 Sistemai serveryje išskirtas kietojo disko dydis turi būti ne mažesnis nei 10 GB.

NAR-2 Sistema turi pateikti sistemos naudotojui užklausos rezultatus ne ilgiau nei per 2 sekundes (išskyrus grėsmių vizualizavimo įrankį).

NAR-3 Pagal galimybes įstaigoje nuo serverio, kuriame veikia grėsmių vizualizavimo prototipas iki sistemos naudotojų rekomenduojama tinklo mazgus sujungti optiniais kabeliais dėl spartesnio tinklo ryšio pralaidumo.

NAR-4 Serveris, kuriame įdiegtas grėsmių vizualizavimo prototipas, turi gebeti aptarnauti ne mažiau nei 100 aktyvių vartotojų.

NAR-5 Serverio, kuriame įdiegtas grėsmių vizualizavimo prototipas, ir sistemos naudotojų aparatinė dalis ne prastesnė nei 2 GHz procesorius, 1 GB operatyvios atminties, 30GB kietasis diskas.

4.1.3.13. Diegimo reikalavimai

4.1.3.14. Ruošinio reikalavimai

DRR-1 Sistemos ruošinys turi būti pateiktas 700 MB standartiname kompaktiniame diske (CD).

DRR-2 Ruošinio kompaktiniame diske turi būti keliais formatais pateikta sistemos archyvuota rinkmena su pirminiu programos tekstu bei sistemos duomenų bazės atvaizdas SQL formatu su testiniais duomenimis.

DRR-3 Ruošinio kompaktiniame diske turi būti pateikta ruošinio reikalavimų specifikacija.

4.1.3.15. Instaliavimo reikalavimai

INR-1 Pagal OSNR reikalavimus tinkamai sukonfigūruota aplinka su nustatyta interneto serverio numatytuoju pradžios katalogu.

INR-2 Numatyjame pradžios kataloge išarchyvuoti sistemos pirmąjį programos tekstą ir išarchyvuotoje konfigūracinėje rinkmenoje įrašyti duomenų bazės vartotojo prisijungimo duomenis.

INR-3 Naudojant sistemos duomenų bazės atvaizdą sukurti duomenų bazę.

4.1.3.16. Pradinio duomenų bazių kaupimo reikalavimai

PDBKR-1 Duomenų bazės kurti nereikia, ji bus automatiškai sukurta į duomenų bazės valdymo sistemą įkėlus sistemos duomenų bazės atvaizdą.

PDBKR-2 Duomenų bazės vartotojui turi būti suteikta teisė kurti naujas lenteles ir jas trinti.

4.1.3.17. Sistemos įsisavinimo reikalavimai

SIR-1 Vartotojas suprantantis MVC projektavimo sprendimą (angl. *design pattern*), kuris leidžia atsieti prieigą prie duomenų ir verslo logiką nuo būdo, kuriuo jis rodomas vartotojui [39] bei Three.js supaprastintą daugianaršyklinę „JavaScript“ biblioteką/API skirtą kurti ir atvaizduoti animuotą kompiuterinę grafiką interneto naršyklėje [40] veikimo principus, turėtų įsisavinti sistemą ne ilgiau kaip per vieną savaitę.

4.1.3.18. Aptarnavimo ir priežiūros reikalavimai

Aptarnavimo ir priežiūros reikalavimų nenumatyta.

4.1.3.19. Tiražuojamumo reikalavimai

Tiražuojamumo reikalavimų nenumatyta.

4.1.3.20. Apsaugos reikalavimai

AR-1 Sistemos apsaugą užtikrina įstaigos struktūrinis padalinys atsakingas už sistemos diegimą ir tolesnius jos atnaujinimus bei kiti už sistemą saugumą atsakingi įstaigos darbuotojai.

AR-2 Sistemos panaudojimui įstaiga turi paskirti sistemos administratorių, kitus sistemos naudotojus, sistemos saugumo įgaliotinį ir parengti procedūras saugiam sistemos eksplotavimui.

AR-3 Sistemos administratorius atlieka sistemos priežiūrą, apmoko sistemos naudotojus, suteikia jiems prisijungimo duomenis prie sistemos techninių išteklių pagal jų darbo specifiką ir įstaigos įpareigojimus.

4.1.3.21. Juridiniai reikalavimai

JUR-1 Sistemos kūrimo ir tolesnio eksplotavimo metu draudžiama sistemoje diegti kenkėjišką programos kodą, kuris galėtų kelti grėsmę įstaigos vertybėms.

JUR-2 Sistemoje negali būti naudojami komponentai, kurie galėtų pažeisti kitų autoriu teises pagal Autorių teisių ir gretutinių teisių įstatymą.

JUR-3 Sistemoje siekiant saugoti asmens duomenis, turi būti suderinti teisės aktai pagal Asmens duomenų teisinės apsaugos įstatymą.

4.2. Grėsmių vizualizavimo prototipo bandymai

Pagal reikalavimų specifikaciją sistema įdiegta ir paleista kompiuterio virtualioje mašinoje, o bandymai atliekami iš vietinio kompiuterio. Sistemos bandymams naudojamasi iš anksto paruoštomis sistemos administratoriaus, informacijos saugumo grupės ir vertybų priežiūros grupės GVSR-2 vartotojo sąsajomis.

4.2.1. GVSRU-1 užduoties bandymas

Bandymas pagal UFBR-1 reikalavimą atliekamas su kiekvienu sistemos naudotojo vaidmeniu. Interneto naršykle prisijungjama prie sistemos lokaliamo kompiuterio tinklo adresu <http://magistras.vgtu.lt>, įvedami prisijungimo duomenys ir spaudžiamas prisijungimo mygtukas.

Bandymo metu įvedus prisijungimo duomenis ir paspaudus mygtuką „Toliau“ sistemos administratorius nukreipiamas į „Administratoriai“ meniu skyrių, informacijos saugumo grupė – „Rizikos valdymo“ skyrių, vertybų priežiūros grupė – „Įstaigos“ skyrių. Prisijungus prie sistemos atvaizduojama GVSR-2 vartotojo sąsaja, matosi sistemos naudotojui priskirti skyriai, logotipas, naudotojo informacija, kalbos nustatymai ir atsijungimo mygtukas. Atsijungiant sistema nukreipia į prisijungimo prie sistemos langą GVSR-1.

4.2.2. GVSRU-2 užduoties bandymas

Bandymas pagal UFBR-2 reikalavimą atliekamas su sistemos administratoriaus vaidmeniu prisijungus prie sistemos pagal GVSRU-1 prisijungimo aprašą. Renkantis „Administratoriai“ meniu skyrių vartotojo lange atvaizduojamas ULMSR-1 langas, kuriamo pateiktas sistemos naudotojų sąrašas.

Spaudžiant sistemos naudotojo ištrynimo mygtuką UPR-3 pasirinktas sistemos naudotojas ištrinamas ir atnaujinama sistemos naudotojų sąrašo informacija.

Spaudžiant ULMSR-1 veiksmų mygtuką „Sukurti“ sistemoje atvaizduojamas ULMDR-1 lango maketas su sistemos naudotojo duomenų įvesties laukais. Bandant spausti ULMDR-1 veiksmų mygtuką „Išsaugoti“ perkraunamas langas, kuriamo atvaizduojamas klaidos pranešimas su paaiškinimais. Įvedus vartotojo vardą, slaptažodį, nustačius sistemos naudotojo vaidmenį ir pakartotinai spausdus šią mygtuką vartotojo sąsaja nukreipiama į sistemos naudotojų sąrašą, kuris buvo papildytas nauju prieš tai aprašytu sistemos naudotoju.

Spaudžiant ULMSR-1 piktogramą UPR-2 sistemoje atvaizduojamas ULMDR-1 to paties kaip ir sukūrimo metu duomenų įvedimo langas su iš anksto užpildytais laukais. Pakeitus sistemos naudotojo vaidmenį spaudžiamas ULMDR-1 veiksmų mygtukas „Išsaugoti“ vartotojo sąsaja nukreipiama į sistemos naudotojų sąrašą, kuriamo matosi, kad pasirinktas sistemos naudotojas turi kitą sistemos naudotojo vaidmenį.

4.2.3. GVSRU-3 užduoties bandymas

Bandymas pagal UFBR-3 reikalavimą atliekamas su vertybų priežiūros grupės nario vaidmeniu prisijungus prie sistemos pagal GVSRU-1 prisijungimo aprašą. Bandymo metu sistemoje sukuriame Vilniaus Gedimino technikos universiteto, kelių jo fakultetų ir objektų (pavyzdžiui auditorijos) bandymo duomenų įrašai. Šiam tikslui naudojamas „Įstaigos“ meniu skyrius.

Spaudžiant „Įstaigos“ meniu poskyrį atvaizduojamas ULMSR-2 langas, kuriamo pateikiamas įstaigų sąrašas. Iš įstaigos formą įvedame įstaigos pavadinimą (pavyzdžiui „VGTU“) ir spaudžiame mygtuką „Išsaugoti“. Sistema prideda universiteto įrašą prie įstaigų sąrašo.

Spaudžiant „Struktūrinių padalinių sąrašas“ meniu poskyrį atvaizduojamas ULMSR-1 langas, kuriamo pateikiamas pilnas įstaigų ir jų struktūrinių padalinių bei objektų sąrašas. Spaudžiant mygtuką „Sukurti“ atvaizduojamas ULMDR-1 duomenų įvedimo langas. Pasirenkama atitinkama įstaiga (pavyzdžiui „VGTU“) ir įvedamas jos struktūrinis padalinys

(pavyzdžiui „Fundamentinių mokslų fakultetas“), spaudžiamas mygtukas „Išsaugoti“. Analogiškai kuriami kiti struktūrinių padalinijų įrašai.

Spaudžiant „Objektai“ meniu poskyrių atvaizduojamas ULMSR-1 langas, kuriamo pateikiamas pilnas objektų sąrašas. Spaudžiant „Sukurti“ mygtuką atvaizduojamas ULMDR-1 duomenų įvedimo langas. Pasirenkamas struktūrinis padalinys (pavyzdžiui „Fundamentinių mokslų fakultetas“) ir įvedamas objekta pavadinimas (pavyzdžiui „417, I LK“). Analogiškai kuriami kiti objektų įrašai.

Pagal UFBR-3 reikalavimą duomenų keitimo ir šalinimo veiksmai taip pat sėkmingai išbandyti. Duomenų keitimas vyksta panašiai kaip ir duomenų sukūrimas. Esminis skirtumas tik tas, kad reikia prie atitinkamų duomenų juostos spausti UPR-2 piktogramą. Duomenų šalinimui reikia pažymėti atitinkamus laukus ir spausti mygtuką „Pašalinti“. Įstaigos meniu poskyryje redaguoti duomenų negalima, galima tik šalinti duomenis paspaudus atitinkamą UPR-3 piktogramą.

„Įstaigos“ meniu skyriaus ULMSR-1 langas pateiktas (žr. 15 pav.).

Nr.	Istaiga	Struktūrinių padalinys	Padalinio adresas	N. obj.	Pozicija	Statusas	
1.	VGTU	Elektronikos fakultetas	Naugarduko g. 41, Vilnius	+ <input checked="" type="checkbox"/>	1 <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2.	VGTU	Fundamentinių mokslų fakultetas	Saulėtekio al. 11, Vilnius	+ <input checked="" type="checkbox"/>	2 <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

15 pav. „Įstaigos“ meniu skyriaus „Struktūrinių padalinijų sąrašas“ poskyris

4.2.4. GVSRU-4 užduoties bandymas

Bandymas pagal UFBR-4 reikalavimą atliekamas su vertybų priežiūros grupės nario vaidmeniu prisijungus prie sistemos pagal GVSRU-1 prisijungimo aprašą. Bandymo metu sistemoje sukuriama universiteto objektuose saugomų vertybų bandymo duomenų įrašai. Šiam tikslui naudojamas „Vertybės“ meniu skyrius.

Spaudžiant „Vertybės“ meniu poskyrių atvaizduojamas ULMSR-1 langas, kuriamo pateikiamas detalus vertybų sąrašas. Spaudžiant mygtuką „Sukurti“ atvaizduojamas ULMDR-1

duomenų įvedimo langas. Pasirenkama atitinkama vertybės rūšis (pavyzdžiu „Diskelis“) ir įvedamas vertybės pavadinimas (pavyzdžiu „1.44 MB Floppy Disk“), spaudžiamas mygtukas „Išsaugoti“. Analogiskai kuriami kiti vertybių įrašai.

Spaudžiant „Grupė“ meniu poskyrį atvaizduojamas ULMSR-1 langas, kuriamo pateikiamas vertybių grupių sąrašas. Spaudžiant mygtuką „Sukurti grupę“ atvaizduojamas ULMRD-1 duomenų įvedimo langas. Įvedama atitinkama vertybės grupė (pavyzdžiu „Kompiuterinė įranga“), spaudžiamas mygtukas „Išsaugoti“. Analogiskai kuriami kiti vertybių grupių įrašai.

Spaudžiant „Rūšis“ meniu poskyrį atvaizduojamas ULMSR-1 langas, kuriamo pateikiamas vertybių rūšių sąrašas. Spaudžiant „Sukurti rūši“ mygtuką atvaizduojamas ULMRD-1 duomenų įvedimo langas. Pasirenkama atitinkama vertybės grupė (pavyzdžiu „Kompiuterinė įranga“) ir įvedama vertybės rūsis (pavyzdžiu „Kompiuteris“). Analogiskai kuriami kiti vertybių rūšių įrašai.

Pagal UFBR-4 reikalavimą duomenų keitimo ir šalinimo veiksmai taip pat sėkmingai išbandyti. Duomenų keitimas vyksta panašiai kaip ir duomenų sukūrimas. Esminis skirtumas tik tas, kad reikia prie atitinkamų duomenų juostos spausti UPR-2 piktogramą. Duomenų šalinimui reikia pažymeti atitinkamus laukus ir spausti mygtuką „Pašalinti“.

„Vertybės“ meniu poskyrio ULMSR-1 langas pateiktas (žr. 16 pav.).

Vertybės							
Vertybės							
<input type="button" value="Viso: 11"/> <input type="button" value="300"/> <input type="button" value="Naujų puslapyje"/> <input type="button" value="1"/> <input type="button" value="Sukuri"/> <input type="button" value="Pašalinti"/>							
Nr.	Grupė	Rūsis	Pavadinimas	Pastabos	Kiekis	Statusas	<input type="checkbox"/>
1.	Kompiuterinė įranga	Kompiuteris	LENOVO ThinkCentre M58e		3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.	Kompiuterinė įranga	Nėštojamas kompiuteris	DELL Inspiron 15.6" Touch-Screen Laptop		0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3.	Kompiuterinė įranga	Serveris	LENOVO ThinkCentre M73		1	<input type="checkbox"/>	<input type="checkbox"/>
4.	Kompiuterinė įranga	Monitorius	DELL monitorius		2	<input type="checkbox"/>	<input type="checkbox"/>
5.	Kompiuterinė įranga	Klaviatūra	LENOVO keyboard		2	<input type="checkbox"/>	<input type="checkbox"/>
6.	Kompiuterinė įranga	Pelė	LENOVO mouse		2	<input type="checkbox"/>	<input type="checkbox"/>
7.	Kompiuterinė įranga	Skaitlytuvas	HP Scanjet 200		1	<input type="checkbox"/>	<input type="checkbox"/>
8.	Buro įranga	Kondicioneerius	Eledra JED 18 DCI 796		1	<input type="checkbox"/>	<input type="checkbox"/>
9.	Laišmenos	Diskelis	1.44MB Floppy Disk		0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10.	Baldai	Stalas	Darvin		2	<input type="checkbox"/>	<input type="checkbox"/>
11.	Baldai	Kėdė	ALRIK sukausoji		2	<input type="checkbox"/>	<input type="checkbox"/>

16 pav. „Vertybės“ meniu skyriaus „Vertybės“ poskyris

4.2.5. GVSRU-5 užduoties bandymas

Bandymas pagal UFBR-5 reikalavimą atliekamas su vertybų priežiūros grupės nario vaidmeniu prisijungus prie sistemos pagal GVSRU-1 prisijungimo aprašą. Bandymo metu sistemoje sukuriami universiteto inventoriaus įrašai, kurie apjungia vertybės buvimo vietas ir pačio vertybės informaciją. Šiam tikslui naudojamas „Inventorius“ meniu skyrius.

Spaudžiant „Inventorius“ meniu poskyrį atvaizduojamas ULMSR-3 langas, kuriame pateikiamas detalus įstaigų inventoriaus sąrašas. Spaudžiant mygtuką „Sukurti įrašą“ atvaizduojamas ULMDR-1 duomenų įvedimo langas. Pasirenkama atitinkama vertybės buvimo vieta (pavyzdžiu „VGTU Fundamentinių mokslų fakultetas 417, I LK“) ir vertybė (pavyzdžiu „Diskelis 1.44 MB Floppy Disk“), spaudžiamas mygtukas „Išsaugoti“. Analogiškai kuriami kiti įstaigos inventoriaus įrašai.

Pagal UFBR-5 reikalavimą duomenų keitimo ir šalinimo veiksmai taip pat sėkmingai išbandyti. Duomenų keitimas vyksta panašiai kaip ir duomenų sukūrimas. Esminis skirtumas tik tas, kad reikia prie atitinkamų duomenų juostos spausti UPR-2 piktogramą. Duomenų šalinimui reikia pažymeti atitinkamus laukus ir spausti mygtuką „Pašalinti“.

„Inventorius“ meniu poskyryje funkcionuoja duomenų paieška, kuri leidžia pasirinkti duomenis tarp pasirinktų įstaigų ir (arba) vertybės, serijinio numerio, inventorinio numerio, įsigyjimo datos, perdavimo datos įrašų.

„Inventorius“ meniu poskyrio ULMSR-3 langas pateiktas (žr. 17 pav.).

The screenshot shows the 'Inventorius' menu interface. At the top, there are tabs for 'Įstaigos', 'Inventorius', and 'Vertybės'. Below these are sub-tabs: 'Inventorius', 'Periferijos sąrašas', 'Nauji', and 'Istorija'. A search bar displays 'Viso: 10' and '200' with a dropdown menu showing '... Pasirinkti ...' and 'Pridėti papildoma padalinį'. On the right, there are two sets of radio buttons for 'ARBA' and 'IR'. Under 'Paleška:', there are dropdown menus for 'Vertybė' containing 'LENOVO' and 'DELL', and another dropdown for 'Pridėti papildoma paleškos lauką'. Below the search area is a table with the following data:

Nr.	Įstaiga ir padalinys	Objektas	Vertybė	Veliuntinis / Sugedęs	Sertifikatas Nr.	Inventorius Nr.	Perdavimo data	Garantinis laikotarpis			
1.	VGTU Fundamentinių mokslų fakultetas	417, I LK	DELL monitorius	DELL10212	1343				<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.	VGTU Fundamentinių mokslų fakultetas	417, I LK	DELL monitorius	DELL10211	1342			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
3.	VGTU Fundamentinių mokslų fakultetas	417, I LK	LENOVO keyboard	AB100BK119A	1344A			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
4.	VGTU Fundamentinių mokslų fakultetas	417, I LK	LENOVO keyboard	AB100BK200A	1345A			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
5.	VGTU Fundamentinių mokslų fakultetas	417, I LK	LENOVO mouse	AB100BK119B	1344B			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
6.	VGTU Fundamentinių mokslų fakultetas	417, I LK	LENOVO mouse	AB100BK200B	1345B			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

17 pav. „Inventorius“ meniu skyriaus „Inventorius“ poskyris

4.2.6. GVSRU-6 užduoties bandymas

Bandymas pagal UFBR-6 reikalavimą atliekamas su informacijos saugumo grupės nario vaidmeniu prisijungus prie sistemos pagal GVSRU-1 prisijungimo aprašą. Bandymo metu sistemoje sukuriami grėsmių šaltinių, grėsmių, pažeidžiamumų įrašai bei grėsmių ir pažeidžiamumų grupės bus priskirtos pagal vertėbes arba įstaigų struktūrą. Šiam tikslui naudojamas „Rizikos valdymo“ meniu skyrius.

Spaudžiant „Grėsmių sąrašas“ meniu poskyrių atvaizduojamas ULMSR-4 langas, kuriami pateikiamas detalus grėsmių šaltinių ir grėsmių sąrašas. Spaudžiant mygtuką „Sukurti naują grėsmių šaltinį“ atvaizduojamas ULMDR-1 duomenų įvedimo langas. Įvedamas grėsmės šaltinis (pavyzdžiui „Žmogus / tyčiniai“), spaudžiamas mygtukas „Išsaugoti“. Analogiškai kuriami kiti grėsmių šaltinių įrašai. Spaudžiant mygtuką „Sukurti naują grėsmę“ atvaizduojamas ULMDR-1 duomenų įvedimo langas. Pasirenkami atitinkami grėsmių šaltiniai (pavyzdžiui „Žmogaus / atsitiktiniai“ ir „Žmogaus / tyčiniai“) ir įvedamas grėsmės pavadinimas (pavyzdžiui „Duomenų praradimas“), spaudžiamas mygtukas „Išsaugoti“. Analogiškai kuriami kiti grėsmių įrašai. Pasirenkant atitinkamą kiekį grėsmių įrašų galima spausti mygtuką „Sukurti pažeidžiamumą pasirinktai grėsmei“. Sistema atvaizduos ULMDR-1 duomenų įvedimo langą, kuriami galima įvesti pasirinktą grėsmių pažeidžiamumą (pavyzdžiui „Darbuotojai atliekantys atsargines duomenų kopijas jas atliks netinkamai ir sugadins duomenis“). Analogiškai kuriami kiti pažeidžiamumų įrašai.

Spaudžiant „Pažeidžiamumų sąrašas“ meniu poskyrių atvaizduojamas ULMSR-5 langas, kuriami pateikiamas detalus pažeidžiamumų sąrašas su pagal nutylėjimą numatytomis grėsmės pasireiškimo tikimybės ir poveikio reikšmėmis. Siekiant keisti grėsmės pasireiškimo tikimybės ir poveikio reikšmes pasirenkame atitinkamą pažeidžiamumą (pavyzdžiui „Darbuotojai atliekantys atsargines duomenų kopijas jas atliks netinkamai ir sugadins duomenis“) ir parenkame grėsmės tikimybę (pavyzdžiui „Maža“) ir poveikį (pavyzdžiui „Didelė“). Analogiškai nustatomi kitų grėsmių ir pažeidžiamumų grupių grėsmės pasireiškimo tikimybės ir poveikio reikšmės pagal nutylėjimą.

Pagal UFBR-6 reikalavimą duomenų keitimo ir šalinimo veiksmai taip pat sėkmingai išbandyti. Duomenų keitimas vyksta panašiai kaip ir duomenų sukūrimas. Esminis skirtumas tik tas, kad reikia prie atitinkamų duomenų juostos paspausti UPR-2 piktogramą. Duomenų šalinimui reikia pažymeti atitinkamus laukus ir spausti mygtuką „Pašalinti“.

Spaudžiant „Priskyrimas“ meniu poskyrių atvaizduojamas ULMSR-6 langas, kuriami pateikiamas grėsmių ir pažeidžiamumų grupių sąrašas su priskyrimo prie vertėbių ar jų buvimo

vietos nustatymais. Siekiant papildyti nustatymus prie atitinkamo pažeidžiamumo (pavyzdžiu „Darbuotojai atliekantys atsargines duomenų kopijas jas atliks netinkamai ir sugadins duomenis“) nustatome, kuriami vertybų būvimo vietoje šis pažeidžiamumas gali pasireikšti (pavyzdžiu „417, I LK“ ir „418, I LK“). Šiuos nustatymus galima priskirti grėsmių ir pažeidžiamumų grupėms pagal vertybes ir jų požymius arba pagal įstaigas ir jų padalinius ir (ar) objektus. Prie grėsmių ir pažeidžiamumų grupių priskirti įrašai šalinami spaudžiant UPR-3 piktogramą individualiems įrašams arba pasirinkus grėsmių ir pažeidžiamumų grupes ir spaudžiant mygtuką „Pašalinti“, taip bus pašalinti visi priskyrimai prie pasirinktų grėsmių ir pažeidžiamumų grupių.

„Priskyrimas“ meniu poskyryje funkcionuoja grėsmių ir pažeidžiamumų grupių filtravimas, kuris leidžia pasirinkti atitinkamas grėsmių ir pažeidžiamumų grupes pagal grėsmių arba grėsmių šaltinių sąrašą.

„Priskyrimas“ meniu poskyrio ULMSR-6 langas pateiktas (žr. 18 pav.).

Nr.	Grėsmės salinis	Grėsmė	Pazeidžiamumas	Įstaiga	Padalinys	Objektas	Bausgėti	Padalinti
1.	Zmogaus / atstikliniai Zmogaus / tydinai	Duomenų pradidamas	Darbuotojai atliekantys sistemų atsargines kopijas jas atliks netinkamai ir sugadins atsarginius duomenis			X417, I LK X418, I LK	<input type="checkbox"/>	<input type="checkbox"/>
2.	Zmogaus / atstikliniai Zmogaus / tydinai	Kenčiantis programinis kodas	Ne visuose kompiuteriuose yra naudojama antivirusinė programa.			XElektronikos fakultetas	<input type="checkbox"/>	<input type="checkbox"/>
3.	Zmogaus / atstikliniai Zmogaus / tydinai	Ginkluoti asmenys	Nėra asmenų patikros palenkant į patalpas.	XVGTU		X427, I LK	<input type="checkbox"/>	<input type="checkbox"/>

18 pav. „Rizikos valdymas“ meniu skyriaus „Priskyrimas“ poskyris

4.2.7. GVSRU-7 užduoties bandymas

Bandymas pagal UFBR-7 reikalavimą atliekamas su informacijos saugumo grupės nario vaidmeniu prisijungus prie sistemos pagal GVSRU-1 prisijungimo aprašą. Bandymo metu sistemoje apibréžiami kylančių grėsmių ir rizikos parametrai, kurie pagal įstaigoje disponuojamų vertybų kritiškumo požymius suformuoja rizikos matricą, skirtą vertinti ir tvarkyti riziką bei vizualizuoti kritines grėsmes. Šiam tikslui naudojamas „Rizikos valdymo“ meniu skyrius.

Spaudžiant „Nustatymai“ meniu poskyrį atvaizduojamas ULMSR-7 langas, kuriami detaliai pateikiama vertybėms kylančių grėsmių ir pažeidžiamumų grupių poveikio, tikimybės ir rizikos parametrai. Grėsmės ir pažeidžiamumo grupių tikimybės, poveikio ar rizikos

pasireiškimo nauji parametrai sukuriami spaudžiant UPR-7 piktogramą. Po paspaudimo pagal pasirinkimą atvaizduojamas ULMDR-1 duomenų įvedimo langas. Siekiant sukurti grėsmės ir pažeidžiamumo grupės pasireiškimo naują poveikio ar tikimybės įrašą įvedamas poveikį ar tikimybę nusakantis dydis žodine ir skaitine reikšme (pavyzdžiu „Maža“, „10.0“) ir spaudžiamas mygtukas „Išsaugoti“. Analogiskai kuriami kiti grėsmės ir pažeidžiamumo grupės pasireiškimo poveikio ir tikimybės įrašai. Grėsmės ir pažeidžiamumo grupės pasireiškimo rizikos parametru aprašyti būtina įvesti riziką nusakančių dydžių žodine ir skaitine, nusakyta intervalo režiuose, reikšme bei pasirenkamas spalvos kodas, kuris sistemoje, rizikos valdymo ataskaitose ir vizualizacijose nusakys apibrėžtą rizikos dydi.

Pagal UFBR-7 reikalavimą duomenų keitimo ir šalinimo veiksmai taip pat sėkmingai išbandyti. Duomenų keitimas vyksta „Nustatymai“ meniu poskyryje atitinkamai keičiant tikimybės, poveikio ir rizikos paremtrų žodines ar skaitines reikšmes ir spaudžiant mygtuką „Išsaugoti“. Duomenų įrašui pašalinti prie atitinkamos tikimybės, poveikio ar rizikos paremtrų spaudžiama piktograma UPR-3.

Sukuriant naujus įrašus, keičiant įrašų duomenis, ar juos šalinant „Nustatymai“ meniu poskyryje atitinkamai kinta rizikos matrica, kuri gaunama grėsmės ir pažeidžiamumo pasireiškimo tikimybę dauginant iš jo sukeliamo poveikio.

„Nustatymai“ meniu poskyrio ULMSR-7 langas pateiktas (žr. 19 pav.).

Rizikos valdymas	Grėsmių sąrašas	Pažeidžiamumu sąrašas	Priskyrimas	Nustatymai																															
Rizikos valdymas																																			
Nustatymų administruavimas																																			
Išsaugoti																																			
Rizikos matrica	<table border="1"> <thead> <tr> <th colspan="3">Grėsmės tikimybė</th> <th>Grėsmės poveikis</th> </tr> <tr> <th></th> <th>Maža 10.0</th> <th>Vidutinė 50.0</th> <th>Didelė 100.0</th> </tr> </thead> <tbody> <tr> <td>Didelė 1.0</td> <td>Maža$10.0 * 1.0 = 10$</td> <td>Vidutinė$50.0 * 1.0 = 50$</td> <td>Didelė$100.0 * 1.0 = 100$</td> </tr> <tr> <td>Vidutinė 0.5</td> <td>Maža$10.0 * 0.5 = 5$</td> <td>Vidutinė$50.0 * 0.5 = 25$</td> <td>Vidutinė$100.0 * 0.5 = 50$</td> </tr> <tr> <td>Maža 0.1</td> <td>Maža$10.0 * 0.1 = 1$</td> <td>Maža$50.0 * 0.1 = 5$</td> <td>Maža$100.0 * 0.1 = 10$</td> </tr> </tbody> </table>				Grėsmės tikimybė			Grėsmės poveikis		Maža 10.0	Vidutinė 50.0	Didelė 100.0	Didelė 1.0	Maža $10.0 * 1.0 = 10$	Vidutinė $50.0 * 1.0 = 50$	Didelė $100.0 * 1.0 = 100$	Vidutinė 0.5	Maža $10.0 * 0.5 = 5$	Vidutinė $50.0 * 0.5 = 25$	Vidutinė $100.0 * 0.5 = 50$	Maža 0.1	Maža $10.0 * 0.1 = 1$	Maža $50.0 * 0.1 = 5$	Maža $100.0 * 0.1 = 10$											
	Grėsmės tikimybė			Grėsmės poveikis																															
		Maža 10.0	Vidutinė 50.0	Didelė 100.0																															
	Didelė 1.0	Maža $10.0 * 1.0 = 10$	Vidutinė $50.0 * 1.0 = 50$	Didelė $100.0 * 1.0 = 100$																															
Vidutinė 0.5	Maža $10.0 * 0.5 = 5$	Vidutinė $50.0 * 0.5 = 25$	Vidutinė $100.0 * 0.5 = 50$																																
Maža 0.1	Maža $10.0 * 0.1 = 1$	Maža $50.0 * 0.1 = 5$	Maža $100.0 * 0.1 = 10$																																
<table border="1"> <thead> <tr> <th>G r e s m ė s t i k i m y b ē</th> <th>Nr.</th> <th>Pavadinimas</th> <th>Skaitinė vertė</th> <th>+</th> </tr> </thead> <tbody> <tr> <td></td> <td>1.</td> <td>Maža</td> <td>0.1</td> <td>✗</td> </tr> <tr> <td></td> <td>2.</td> <td>Vidutinė</td> <td>0.5</td> <td>✗</td> </tr> <tr> <td></td> <td>3.</td> <td>Didelė</td> <td>1.0</td> <td>✗</td> </tr> </tbody> </table>				G r e s m ė s t i k i m y b ē	Nr.	Pavadinimas	Skaitinė vertė	+		1.	Maža	0.1	✗		2.	Vidutinė	0.5	✗		3.	Didelė	1.0	✗												
G r e s m ė s t i k i m y b ē	Nr.	Pavadinimas	Skaitinė vertė	+																															
	1.	Maža	0.1	✗																															
	2.	Vidutinė	0.5	✗																															
	3.	Didelė	1.0	✗																															
<table border="1"> <thead> <tr> <th>G r e s m ė s p o v e i k i s</th> <th>Nr.</th> <th>Pavadinimas</th> <th>Skaitinė vertė</th> <th>+</th> </tr> </thead> <tbody> <tr> <td></td> <td>1.</td> <td>Maža</td> <td>10.0</td> <td>✗</td> </tr> <tr> <td></td> <td>2.</td> <td>Vidutinė</td> <td>50.0</td> <td>✗</td> </tr> <tr> <td></td> <td>3.</td> <td>Didelė</td> <td>100.0</td> <td>✗</td> </tr> </tbody> </table>				G r e s m ė s p o v e i k i s	Nr.	Pavadinimas	Skaitinė vertė	+		1.	Maža	10.0	✗		2.	Vidutinė	50.0	✗		3.	Didelė	100.0	✗												
G r e s m ė s p o v e i k i s	Nr.	Pavadinimas	Skaitinė vertė	+																															
	1.	Maža	10.0	✗																															
	2.	Vidutinė	50.0	✗																															
	3.	Didelė	100.0	✗																															
<table border="1"> <thead> <tr> <th>Rizika*</th> <th>Nr.</th> <th>Pavadinimas</th> <th>Nuo</th> <th>Iki</th> <th>Rėžiai</th> <th>Spalva</th> <th>+</th> </tr> </thead> <tbody> <tr> <td></td> <td>1.</td> <td>Maža</td> <td>1.0</td> <td>10.0</td> <td>[1.0, 10.0]</td> <td>Green</td> <td>✗</td> </tr> <tr> <td></td> <td>2.</td> <td>Vidutinė</td> <td>10.0</td> <td>50.0</td> <td>(10.0, 50.0]</td> <td>Gold</td> <td>✗</td> </tr> <tr> <td></td> <td>3.</td> <td>Didelė</td> <td>50.0</td> <td>100.0</td> <td>(50.0, 100.0]</td> <td>Red</td> <td>✗</td> </tr> </tbody> </table>				Rizika*	Nr.	Pavadinimas	Nuo	Iki	Rėžiai	Spalva	+		1.	Maža	1.0	10.0	[1.0, 10.0]	Green	✗		2.	Vidutinė	10.0	50.0	(10.0, 50.0]	Gold	✗		3.	Didelė	50.0	100.0	(50.0, 100.0]	Red	✗
Rizika*	Nr.	Pavadinimas	Nuo	Iki	Rėžiai	Spalva	+																												
	1.	Maža	1.0	10.0	[1.0, 10.0]	Green	✗																												
	2.	Vidutinė	10.0	50.0	(10.0, 50.0]	Gold	✗																												
	3.	Didelė	50.0	100.0	(50.0, 100.0]	Red	✗																												

19 pav. „Rizikos valdymas“ meniu skyriaus „Nustatymai“ poskyris

4.2.8. GVSRU-8 užduoties bandymas

Bandymas pagal UFBR-8 reikalavimą atliekamas su informacijos saugumo grupės nario vaidmeniu prisijungus prie sistemos pagal GVSRU-1 prisijungimo aprašą. Bandymo metu sistemoje sukuriama rizikos valdymo ataskaita, atliekamas potencialių grėsmių ir pažeidžiamumų grupių rizikos vertinimas ir tvarkymas. Šiam tikslui naudojamas „Rizikos valdymo“ meniu skyrius.

Spaudžiant „Rizikos valdymas“ meniu poskyrį atvaizduojamas ULMSR-8 langas, kuriame pateikiamas rizikos valdymo ataskaitų sąrašas bei sistemoje naudojami rizikos matricos parametrai. Siekiant sukurti aktualią rizikos valdymo ataskaitą reikia įvesti rizikos valdymo ataskaitos pavadinimą (pavyzdžiui „Rizikos valdymo ataskaita pagal 2016 metų I ketvirčio planą“), pasirinkti jos formavimo būdą (pavyzdžiui „pagal vertybų struktūrą“, „pagal objektų struktūrą“), ir paspausti mygtuką „Pradėti“. Sistema atvaizduoja ULMSR-8 langą su nauju rizikos valdymo ataskaitos įrašu. Prie kiekvienos rizikos valdymo ataskaitos atvaizduojama UPR-3 piktograma, kurią paspaudus ištrina ataskaitą.

Pagal UFBR-8 reikalavimą atliekamas rizikos valdymo ataskaitos duomenų papildymas atliekant rizikos vertinimą. Siekiant atlikti rizikos vertinimą ULMSR-8 lange spaudžiama pasirinktos rizikos valdymo ataskaitos mygtukas „Ataskaitos peržiūra“. Po šio mygtuko paspaudimo saugumo grupės nario vartotojo sasaja nukreipiama į ULMSR-9 langą, kuriame atliekama pasirinktos rizikos valdymo ataskaitos rizikos vertinimas. Rizikos vertinimą saugumo grupės narys atlieka pagal nustatytus grėsmės ir pažeidžiamumo grupių pasireiškimo tikimybės ir poveikio parametrus. Priklausomai nuo rizikos valdymo ataskaitos formavimo būdo rizika vertinama pagal apibrėžtų vertybų struktūrą arba objektų struktūrą. Atlikus grėsmių ir pažeidžiamumų rizikos vertinimą spaudžiamas mygtukas „Atnaujinti“, kurio metu atnaujinamos grėsmės ir pažeidžiamumo grupių pasireiškimo tikimybės ir poveikio duomenys.

„Rizikos valdymo“ meniu poskyrio ULMSR-9 langas rizikos vertinimui pateiktas (žr. 20 pav.).

Administracija	Istogos	Inventorius	Vertybės	Veiksmų	Rizikos valdymas	Saugos vizualizacija								
Rizikos valdymas	Griemiu sąrašas	Pažeidžiamumu sąrašas	Priskrimas	Nustatymai										
Rizikos valdymas														
Rizikos vertinimas - pagal vertybės (inventoriinė)														
Rizikos vertinimas pagal 2016-01-01 planą Nr. 6 (Paulius Narkevičius/2016-01-01)														
Viso: 8	100	Įrašyti puslapje	1			Atnaujinti								
Algal					Rizikos vertinimas (skaičiuojant) Rizikos tvarkymas Atvaizduoti valdymas									
Nr.	Griemės šaltinis Griemė Pažeidžiamumas	Grupės	Griemės tikimybė	Griemės poveikis	Rizika	Rūsys	Griemės tikimybė	Griemės poveikis	Rizika	Rizika	Vertybė	Griemės tikimybė	Griemės poveikis	Rizika
1.	Žmogaus / tyčinių Atsakymo aptarnauti ataka Paskirstyta atsakymo aptarnauti ataka Bus užkištas tinklo mažgas ir neprinicijuojamas pašuaugos internetu.	Kompiuterinė įranga Ryšio įranga	Maža ✓ Maža ✓	Vidutinė ✓ Vidutinė ✓	Maža Maža	Kompiuteris Nešiojamas kompiuteris Serveris Monitorius Klavirtūra Peile Spausdinintuvas Skaitmenis	Maža ✓ Maža ✓	Vidutinė ✓ Vidutinė ✓	Maža Maža Maža Maža Maža Maža Maža	LENOVO ThinkCentre M58e LENOVO mouse LENOVO keyboard LENOVO ThinkCentre M73 DELL Inspiron 15.6" Touch-Screen Laptop DELL monitorius HP Scanjet 200	Didelė ✓ Didelė ✓ Didelė ✓ Didelė ✓ Vidutinė ✓ Vidutinė ✓	Didelė ✓ Didelė ✓ Didelė ✓ Didelė ✓ Vidutinė ✓ Vidutinė ✓	Didelė ✓ Didelė ✓ Didelė ✓ Didelė ✓ Vidutinė ✓ Vidutinė ✓	
2.	Žmogaus / tyčinių Duomenų vystė Sugadinti duomenys Dėl naudojamos pasenusios technologijos neuzlikinamas naudotojų prieglos teisių valdymas istagogos tinkle					Serveris	Vidutinė ✓	Didelė ✓	Vidutinė	LENOVO ThinkCentre M73	Vidutinė ✓	Didelė ✓	Vidutinė	

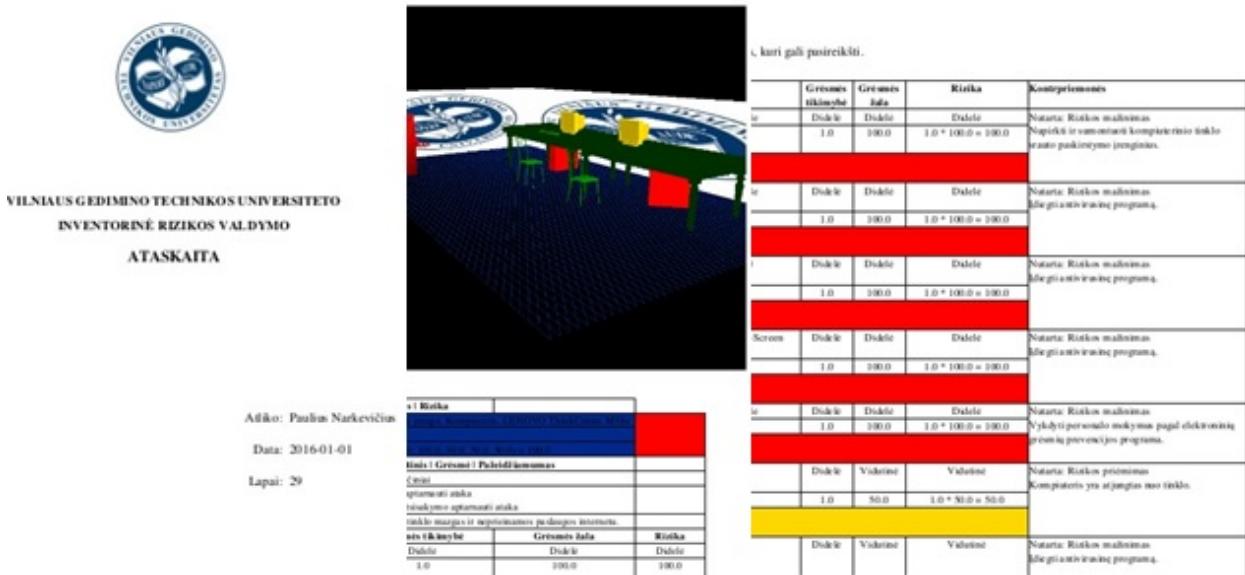
20 pav. „Rizikos valdymas“ meniu skyriaus „Rizikos valdymas“ poskyrio ataskaitos rizikos vertinimas

Po rizikos vertinimo atliekamas rizikos tvarkymas, tam ULMSR-9 lange spaudžiamas mygtukas „Rizikos tvarkymas“. Rizikos tvarkymo metu visos grėsmės ir pažeidžiamumo grupės ULMSR-9 lange išrikiuojamos pagal kylančios grėsmės ir rizikos kritiškumo dydį. Saugumo grupės narys privalo visas grėsmės ir pažeidžiamumo grupes įvertinti ir parinkti tinkamas kontrpriemonės rizikos mažinimui. Po kontrpriemonių pasirinkimo spaudžiamas mygtukas „Atnaujinti“, kurio metu atnaujinama rizikos valdymo ataskaita (žr. 21 pav.).

Rizikos valdymas	Griemiu sąrašas	Pažeidžiamumu sąrašas	Priskrimas	Nustatymai		
Rizikos valdymas						
Rizikos tvarkymas - pagal objektus (organizacinė)						
Rizikos vertinimas pagal 2015-12-16 planą Nr. 5 (Paulius Narkevičius/2015-12-23)						
Viso: 24	100	Įrašyti puslapje	1	Spausdinti ataskaitą Spausdinti ataskaitą Atnaujinti		
Algal				Rizikos vertinimas Rizikos tvarkymas Atvaizduoti valdymas		
Nr.	Griemės šaltinis Griemė Pažeidžiamumas	Pavadinimas	Griemės tikimybė	Griemės poveikis	Rizika	Kontrpriemonės
1.	Žmogaus / atsiliktinių Žmogaus / tyčinių Kenkėjekas programinis kodas Ne visuose kompiuteriuose yra naudojama antivirusinė programa.	Fundamentinių moksly fakultetas	Didelė ✓ 1.0	Vidutinė ✓ 40.0	Vidutinė $1.0 * 40.0 = 40.0$	Rizikos mažinimas Įdiegti antivirusinę.
2.	Žmogaus / atsiliktinių Žmogaus / tyčinių Kenkėjekas programinis kodas Ne visuose kompiuteriuose yra naudojama antivirusinė programa.	417. I LK	Didelė ✓ 1.0	Vidutinė ✓ 40.0	Vidutinė $1.0 * 40.0 = 40.0$	Rizikos priėminimas Atnjungi nuo tinklo rizka priimama.

21 pav. „Rizikos valdymas“ meniu skyriaus „Rizikos valdymas“ poskyrio ataskaitos rizikos tvarkymas

Rizikos tvarkymo metu galima atsispausdinti visą rizikos valdymo ataskaitą PDF ar XLS formatu. Paspaudžiant mygtuką „Spausdinti ataskaitą“ suformuojama rizikos valdymo ataskaita (žr. 22 pav.).



22 pav. Rizikos valdymo ataskaitos spausdinimas PDF formatu

4.2.9. *GVSRU-9 užduoties bandymas*

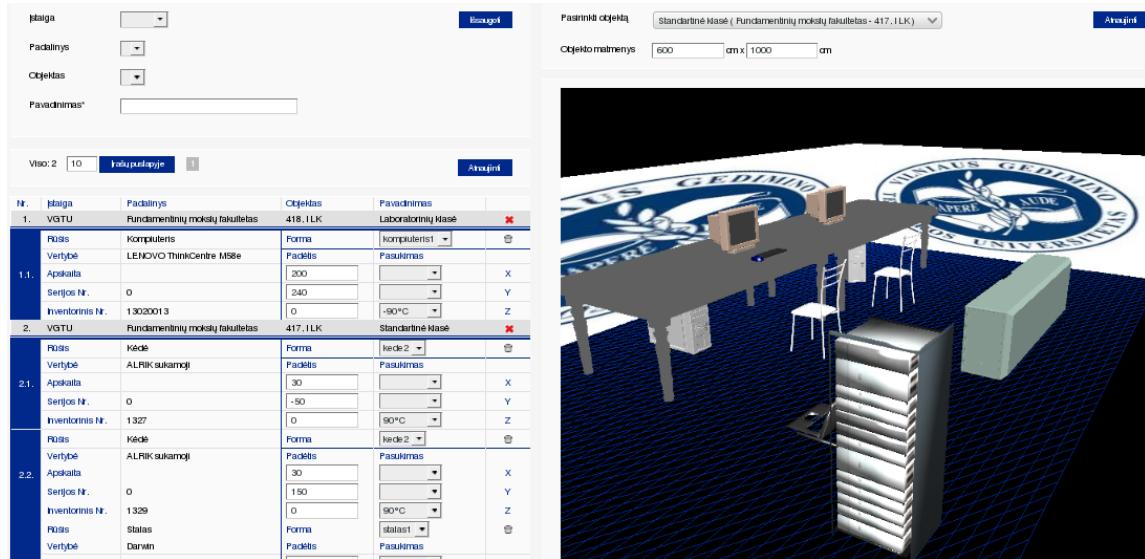
Bandymas pagal UFBR-9 reikalavimą atliekamas su informacijos saugumo grupės nario vaidmeniu prisijungus prie sistemos pagal GVSRU-1 prisijungimo aprašą. Bandymo metu sistemoje apibrėžiama įstaigos objekto trimatė struktūra, kurioje saugomos įstaigos vertybės. Šiam tikslui naudojamas „Saugos vizualizacija“ meniu skyrius.

Spaudžiant „Objektų struktūra“ meniu poskyrį atvaizduojamas ULMSR-10 langas, kuriame pateikiama visa informacija susijusi su įstaigos objektais ir juose esančiomis vertybėmis, ir šių vertybų trimatėmis formomis.

Saugumo grupės narys siekdamas vizualizuoti grēsmes įstaigos objektuose pirmiausiai „Objektų struktūra“ meniu poskyryje sukuria trimatę objekto atvaizdą, t.y. naujo objekto sukūrimo formoje pasirenka įstaigos objekta (pavyzdžiu „VGTU Fundamentinių mokslo fakultetas 417, I LK“) ir įveda šį objektą apibūdinantį pavadinimą (pavyzdžiu „Standartinė auditorija“), ir spaudžia mygtuką „Išsaugoti“. Sukūrus naują objekto atvaizdą atnaujinami objektų sąrašo duomenys. Šiame sąraše pateikiama informacija apie objekto vertybes ir suteikiama galimybė į objektą įtraukti vertybės trimatę formą. Į objektą įtraukus vertybės trimatę formą galima nustatyti šios trimatės formos koordinates ir pasukimo dydį. Po kiekvieno nustatymo pakeitimo spaudžiamas objekto duomenų sąrašo mygtukas „Atnaujinti“. Vertybės

trimatę formą galimą ištrinti spaudžiant UPR-13 piktogramą. Objekto šalinamas spaudžiant UPR-3 piktogramą. Objekto matmenų nustatymo formoje saugumo grupės narys keičia vizualizuojamo objekto ilgio ir pločio parametrus, ir spaudžia mygtuką „Atnaujinti“.

„Objektų struktūra“ meniu poskyrio ULMSR-10 langas pateiktas (žr. 23 pav.).



23 pav. „Saugos vizualizacija“ meniu skyriaus „Objektų struktūra“ poskyris

4.2.10. GVSRU-10 užduoties bandymas

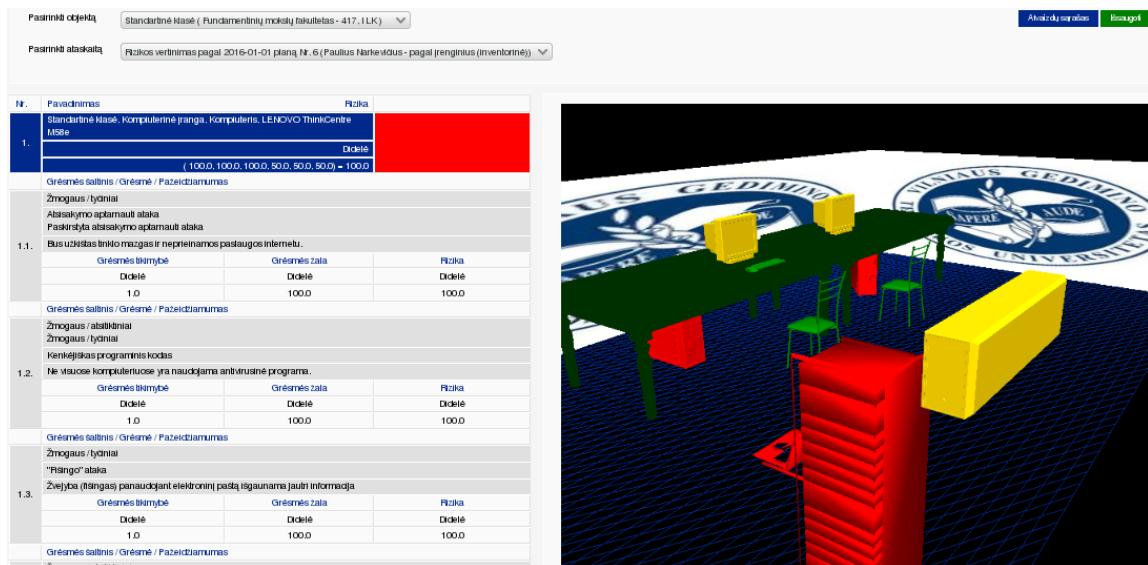
Bandymas pagal UFBR-10 reikalavimą atliekamas su informacijos saugumo grupės nario vaidmeniu prisijungus prie sistemos pagal GVSRU-1 prisijungimo aprašą. Bandymo metu sistemoje vizualizuojamos objekto vertybės pagal rizikos valdymo ataskaitoje atliktus rizikos įvertinimo rezultatus. Šiam tikslui naudojamas „Saugos vizualizacija“ meniu skyrius.

Spaudžiant „Rizikos vizualizavimas“ meniu poskyrių atvaizduojamas ULMSR-11 langas, kuriame pateikiama vizualizuotų įstaigos objektų ir rizikos valdymo ataskaitų sąrašų pasirinkimo langas.

Pasirinkus vizualizuotą įstaigos objektą atvaizduojama trimatė šio objekto vertybų vizualizacija.

Pasirinkus rizikos valdymo ataskaitą atvaizduojamas objektui ir jo vertybėms kylančių grėsmių ir rizikuų sąrašas. Objekto vertybės vizualizuojamos atitinkama spalvų skale pagal grėsmės ir pažeidžiamumo grupių rizikos parametru nustatymus.

„Rizikos vizualizavimas“ meniu poskyrio ULMSR-11 langas pateiktas (žr. 24 pav.).



24 pav. „Saugos vizualizacija“ meniu skyriaus „Rizikos vizualizavimas“ poskyris

4.2.11. GVSRU-11 užduoties bandymas

Bandymas pagal UFBR-11 reikalavimą atliekamas su informacijos saugumo grupės nario vaidmeniu prisijungus prie sistemos pagal GVSRU-1 prisijungimo aprašą. Bandymo metu sistemoje pasirenkamos įvertintos rizikos valdymo ataskaitos ir analizuojami rizikos lygių pokyčiai. Šiam tikslui naudojamas „Rizikos valdymo“ meniu skyrius.

ULMSR-8 lange sužymimos pasirinkimo lauke analizuojamos rizikos valdymo ataskaitos ir spaudžiamas veiksmo mygtukas „Ataskaitų palyginimas“. Sistema užkrauna ULMSR-12 langą pateikiant įstaigos vertybėms kylančių grėsmių ir rizikų sąrašą ir išrikiuojant iš kairės į dešinę ataskaitų rizikos pokyčių rodmenis laiko ašyje nuo anksčiausios ataskaitos iki vėliausios.

„Rizikos valdymo“ meniu poskyrio rizikos valdymo ataskaitų palyginimo rizikos lygiui analizuoti ULMSR-12 langas pateiktas (žr. 25 pav.).

RODYKLĖ								
Nr.	Grėsmės šaltinis Grėsmė Pažeidžiamumas	Rizikos vertinimas pagal 2015-12-13 planą Nr. 1			Rizikos vertinimas pagal 2016-01-01 planą Nr. 2			Rizikos vertinimas pagal 2016-05-27 planą Nr. 3
Polytis	Rizika	Polytis	Rizika	Polytis	Rizika			
1.	Žmogaus / tyčiniai Atsisakymo aptarnauti ataka Paskirstyta atsisakymo aptarnauti ataka Bus užkištas tinklo mazgas ir neprieinamos paslaugos internetu.	▶	Maža (1.0)	⬆	Didelė (100.0)	⬇	Maža (5.0)	➡
2.	Žmogaus / tyčiniai Duomenų vagystė Sugadinti duomenys Dėl naudojamos pasenusios technologijos neužtikrinamas naudotojų prieigos teisių valdymas įstaigos tinkle			⊕	Vidutinė (50.0)		Vidutinė (50.0)	➡
3.	Aplinkos / žmogaus sukelti Gaisras Gaisras, kurį sukėlė aplinkiniai pastatai ar objektai.			⊕	Vidutinė (50.0)	⬇	Maža (5.0)	➡
4.	Žmogaus / atsirkliniai Žmogaus / tyčiniai Kenkėjiskas programinis kodas Ne visuose kompiuteriuose yra naudojama antivirusinė programa.			⊕	Didelė (100.0)	⬇	Vidutinė (50.0)	➡

25 pav. „Rizikos valdymas“ meniu skyriaus „Rizikos valdymas“ poskyrio ataskaitų rizikos lygio palyginimo lentelė

Atitinkamos kylančios grėsmės ir rizikos juosteje paspaudus UPR-20 piktogramą išskleidžiamas vertybų ir (ar) objektų sąrašas su atitinkamais rizikos laipsniais. Vietoje UPR-20 piktogramos atsiranda UPR-21 piktograma, kurią paspaudus išskleistas vertybų ir (ar) objektų sąrašas yra suskleidžiamas. Detalizuotas kylančios grėsmės ir rizikos vertybės pateiktos (žr. 26 pav.).

RODYKLĖ								
Nr.	Grėsmės šaltinis Grėsmė Pažeidžiamumas	Rizikos vertinimas pagal 2015-12-13 planą Nr. 1			Rizikos vertinimas pagal 2016-01-01 planą Nr. 2			Rizikos vertinimas pagal 2016-05-27 planą Nr. 3
Polytis	Rizika	Polytis	Rizika	Polytis	Rizika	Polytis	Rizika	
1.	Žmogaus / tyčiniai Atsisakymo aptarnauti ataka Paskirstyta atsisakymo aptarnauti ataka Bus užkištas tinklo mazgas ir neprieinamos paslaugos internetu.	▶	Maža (1.0)	⬆	Didelė (100.0)	⬇	Maža (5.0)	➡

Kompiuterinė jranga (1.0), Ryšio jranga (1.0), Kompiuteris (1.0), Spausdinčius (1.0), Serveris (1.0), Monitorius (1.0), Nešiojamas kompiuteris (1.0), Nešiojamas kompiuteris (5.0), Klaviatūra (1.0), Pelė (1.0), LENOVO ThinkCentre M58e (1.0), LENOVO mouse (1.0), LENOVO keyboard (1.0), LENOVO ThinkCentre M73 (1.0), DELL Inspiron 15.6" Touch-Screen Laptop (1.0), DELL monitorius (1.0),	Kompiuterinė jranga (5.0), Ryšio jranga (5.0), Kompiuteris (5.0), Spausdinčius (5.0), Serveris (5.0), Monitorius (5.0), Monitorius (5.0), Nešiojamas kompiuteris (5.0), Klaviatūra (5.0), Pelė (5.0), Skaitytuvas (5.0), LENOVO ThinkCentre M58e (100.0), LENOVO mouse (1.0), LENOVO keyboard (1.0), LENOVO ThinkCentre M73 (50.0), DELL Inspiron 15.6" Touch-Screen Laptop (25.0), DELL monitorius (1.0), HP Scanjet 200 (1.0),	Kompiuterinė jranga (5.0), Kompiuteris (5.0), Spausdinčius (5.0), Serveris (5.0), Monitorius (5.0), Nešiojamas kompiuteris (5.0), Klaviatūra (5.0), Pelė (5.0), Skaitytuvas (5.0), LENOVO ThinkCentre M58e (5.0), LENOVO mouse (5.0), LENOVO keyboard (5.0), LENOVO ThinkCentre M73 (5.0), DELL Inspiron 15.6" Touch-Screen Laptop (5.0), DELL monitorius (5.0), HP Scanjet 200 (5.0),
--	---	---

26 pav. „Rizikos valdymas“ meniu skyriaus „Rizikos valdymas“ poskyrio ataskaitų rizikos lygio palyginimo lentelė su detaliu vertybų ir jų rizikos laipsnių sąrašu

4.3. Ketvirto skyriaus apibendrinimas ir pagrindiniai rezultatai

Apibrėžti grėsmių vizualizavimo prototipo techniniai ir programiniai parametrai, nustatyti reikalavimai pagal kuriuos įgyvendintas grėsmių vizualizacijos prototipas. Sukurtas grėsmių vizualizavimo prototipas, kuris leidžia bet kuriuo šio prototipo eksploatavimo metu inicializuoti rizikos valdymo ataskaitos suformavimą, vertinti bei tvarkyti įstaigos vertybėms kylančias grėsmes ir riziką.

Pagal literatūros analizės rezultatus buvo pasirinktas ir įgyvendintas grėsmių vizualizavimas naudojant WebGL technologiją. Grėsmių vizualizavimo taikymo informacijos saugos valdymo procese vizualizavimas pagal metodo eksplikaciją (žr. 10 pav.) realizuotas sukuriant grėsmių vizualizavimo įrankį, kuris leidžia vizualizuoti vertybes pagal informacijos saugos specialisto nustatytais rizikos laipsnių parametrus. Panašiai kaip CySeMoL įrankyje grėsmių vizualizacijos įrankis vizualizuoją įstaigos vertybes pagal joms kylančių grėsmių kritiškumą naudojant rizikos matricos spalvų skalę.

4.3.1. Grėsmių vizualizavimo prototipo privalumai

Galima išskirti tokius sukurto grėsmių vizualizavimo prototipo veikiančio pagal grėsmių vizualizavimo metodą privalumus:

1. informacijos saugumo valdymo procesas netrukdo vertybių priežiūrą atliekančiam personalui, o už informacijos saugumą atsakingi darbuotojai automatiškai gauna vertingą informaciją apie įstaigos vertybių buvimo vietą, kas leidžia kaupti veiklos rezultatus ir numatyti ateities perspektyvas;
2. sistema eksploatuojama kompiuteriniame tinkle, o darbui su prototipo sistema reikalinga tik interneto naršykla, kitos programinės įrangos diegti nereikia, todėl nėra jokių papildomų kaštų;
3. visa sistema gali būti saugoma viename serveryje, todėl supaprastėja sistemos priežiūra;
4. sistemos funkcionalumas išskaidytas naudojant vaidmenimis grindžiamą valdymo sistemą, todėl darbas su sistema yra išskaidytas priklausomai nuo užimamų pareigų įstaigoje;
5. pagreitėja rizikos valdymo procedūra, automatizuojamas ataskaitų suformavimas, sumažėja žmogiškujų išteklių klaidų galimybė ataskaitų rengime, galima lyginti ataskaitas ir matyti kaip pasikeitė situacija nuo pirmosios suformuotos ataskaitos, todėl paprasčiau analizuojami veiklos rezultatai ir pagreitėja sprendimų priėmimo laikas;

- naudojami grėsmių vizualizacijos metodai leidžia lengviau suvokti įstaigoje susidariusią situaciją, įstaigos personalui nereikia daug papildomų informacijos saugumo ar techninių žinių siekiant naudotis prototipo teikiamu funkcionalumu.

4.3.2. Grėsmių vizualizavimo prototipo trūkumai

Galima išskirti tokius sukurto grėsmių vizualizavimo prototipo trūkumus:

- prototipo sistemoje negalima vertybes klasifikuoti pagal turimas savybes, pagal kurias būtų galima priskirti grėsmių ir pažeidžiamumų grupes;
- prototipo sistemoje dar nėra galimybės suformuotų atskirų ataskaitų apjungti į vieną bendrą rizikos valdymo ataskaitą;
- prototipo sistemoje negalima apibrėžti kontrpriemonių sąrašą, kurį būtų galima priskirti vertybėms ir nustatyti atitinkamos kontrpriemonės rizikos mažinimo laipsnį;
- rizikos valdymas atliekamas iš visų sistemos duomenų, nėra galimybės saugumo analizei pasirinkti norimą atskirą įstaigą ar struktūrinį padalinį;
- ne visose kompiuterinės įrangos interneto naršyklėse gali veikti WebGL, nes interneto naršyklės gali blokuoti vaizdo plokštės dėl galimų saugumo spragų;
- grėsmių vizualizacijos procesas išdėstant vertybų formas nėra pakankamai interaktyvus, todėl gaištamas laikas siekiant tinkamai sudėlioti vertybes objekte.

4.4. Ketvirto skyriaus išvados

- Atlikus grėsmių vizualizavimo prototipo projektavimą ir įgyvendinus ši projektą yra nustatyta, kad prototipas veikia pagal aprašytą grėsmių vizualizavimo metodą (žr. 9 pav.), o grėsmių vizualizavimo įrankis – pagal šio metodo eksplikaciją pavaizduotą (žr. 10 pav.). Grėsmių vizualizavimo prototipas leidžia panaudoti skirtingus vizualizavimo metodus: 3D plokštumoje atvaizduojamos vertybės, kurios yra vaizduojamos pagal joms priskirto rizikos laipsnio spalvų skalę; laiko ašyje specialiai simboliais ir pagal spalvų skalę atvaizduojama įstaigos vertybėms kylančių grėsmių ir rizikos pokyčių kaita; galima atsispausdinti PDF rinkmeną, kuri pagal spalvų skalę nuo didžiausios iki mažiausios atvaizduoja kylančių grėsmių ir rizikų sąrašą, o taip pat turi galimybę į šią rinkmeną įtraukti pageidaujamą įstaigos objekto vertybų vizualizaciją su detaliu kylančiu grėsmių ir rizikos sąrašu.

2. Atlikus grėsmių vizualizavimo prototipo bandymus yra nustatyta, kad grėsmių vizualizavimo prototipas veikia pagal grėsmių vizualizavimo prototipo reikalavimų specifikacijoje nustatyti užduočių reikalavimus, o grėsmių vizualizavimo įrankis pagerina informacijos saugos grėsmių vertinimą. 4.3.1. ir 4.3.2. poskyriuose aprašyti pagrindiniai nustatyti grėsmių vizualizavimo prototipo privalumai ir trūkumai.

5. Išvados

1. Atlikus vizualizacija paremtų saugos sistemų projektų ir šiuolaikinių vizualizacijos technologijų analizę nustatyta, kad egzistuoja daug vizualizacija paremtų saugumo sprendimų, kurie skirti informacijos saugumo didinimui, tačiau daug tokių sprendimų yra sudėtingi, brangūs ir reikia specialiai tik tai užduočiai atlikti apmokyto informacijos saugumo personalo. Maža dalis vizualizaciją naudojančių saugumo sprendimų leidžia verslo procesus integruoti kartu su informacijos saugos valdymu, o tai suteiktų galimybę informacijos saugumo valdymui nuolat gauti būtiną pradinę informaciją apie įstaigą ar organizaciją turimas vertybes, kurias būtina apsaugoti. Grėsmių vizualizacijos sprendimai dažnai išsiskiria tuo, kad naudoja spalvų skalę siekiant išskirti grėsmės kritiškumo dydį ir atkreipti dėmesį į pačias pavojingiausias grėsmes, kurias privaloma mažinti norint apsaugoti savo vertybes. Grėsmių vizualizavimas padeda geriau suprasti įstaigai ir jos vertybėms kylančias grėsmes ir riziką. Grėsmių vizualizacija sprendžia informacijos saugos suvaldymo problemą ir apsaugoti turimas vertybes nuo kylančių išorinių ir vidinių grėsmių, ir atitinkamai padėti išsirinkti tinkamas kontrpriemones. Grėsmių vizualizacijos technologijos pasirinkimui, siekiant užtikrinti darbą kompiuteriniame tinkle be papildomo programinės įrangos diegimo, efektyviausias sprendimas būtų panaudoti WebGL vizualizacijos technologiją.
2. Atlikus grėsmių vizualizavimo metodo analizę nustatyta, kad grėsmių vizualizavimui ir įstaigos vertybių rodiklių valdymui užtikrinti geriausiai tinkama panaudoti RBAC naudotojų vaidmenų atskyrimą, o informacijos saugos valdymą užtikrinti su NIST rizikos valdymo metodologija. Grėsmių vizualizavimo metodu įgyvendinti reikia turėti tinkamai nustatytus įstaigos vertybėms kylančios grėsmės ir rizikos laipsnius bei įstaigos objektuose ar patalpose tinkamai apibrėžtas vertybių būvimo vietas. Buvo pasiūlytas šiuos reikalavimus atitinkantis grėsmių vizualizavimo metodas pagal kurį buvo kuriamas grėsmių vizualizavimo prototipas. Pasiūlytas vizualizavimo metodas leidžia nustatyti įstaigos ar organizacijos vertybių geolokaciją ir apibrėžti šioms vertybėms kylančių grėsmių ir rizikos laipsnį.
3. Atlikus grėsmių vizualizacijos prototipo realizaciją nustatyta, kad vizualizavimas pagerina informacijos saugos grėsmių vertinimą ir leidžia kritiškiau vertinti ir atskirti vertybes, kurioms turi būti skiriama ypač didelis dėmesys informacijos saugumui stiprinti nuo tų, kurios yra mažiau pažeidžiamos. Sukurtas grėsmių vizualizavimo

prototipas leidžiantis valdyti įstaigos vertybes bei užtikrinti jų informacijos saugumą vykdant rizikos valdymo procedūras. Sėkmingai įgyvendintas grėsmių vizualizavimo metodas ir išbandytas grėsmių vizualizacijos įrankis. Tačiau yra dar daug galimybių, kaip būtų galima patobulinti grėsmių vizualizavimo prototipą integrnuojant į jį daugiau informacijos saugos įrankių ir kitą funkcionalumą, nurodytą tolesnių darbų poskyryje.

4. Sukurto prototipo galutinė versija bus pristatyta Lietuvos Respublikos Nacionalinei komunikacijų apsaugos tarnybai ir Saugumo priežiūros tarnybai, ir aptarta galimybė pritaikyti ar panaudoti šį prototipą valstybinio sektoriaus įstaigų vertybių ir rizikos valdymo optimizavimui.

Tolesni darbai

*Latest changes:

(Author finished the Project in 2016-2017)

(Author got Masters Diploma in 2016-2017)

(Author dropped the Project out in 2018-2019)

(The Project will be trashed out in 2021-2023)

6. Literatūros sąrašas

1. *Engineering Principles for Information Technology Security* [interaktyvus]. 2014. NIST Special Publication 800-27 Rev A [žiūrėta 2014 m. birželio 14 d.]. Prieiga per internetą: <<http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf>>
2. Vasilecas, O.; Čenys, A.; Sosunovas, S.; Goranin, N. 2008. *Informacinių sistemų sauga*. Vilnius: Technika. 274 p. ISBN 9789955282532.
3. *Assets, Threats and Vulnerabilities: Discovery and Analysis* [interaktyvus]. 2014. Symantec Corporation [žiūrėta 2014 m. birželio 14 d.]. Prieiga per internetą: <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Risk_Management.pdf>
4. Nusinok, M. 2009. Visualizing Threat and Impact Assessment to Improve Situation Awareness, in Proc. *Military Communications Conference, 2009. MILCOM 2009* [interaktyvus]. [žiūrėta 2014 m. birželio 14 d.]. Prieiga per internetą: <<https://ritdml.rit.edu/bitstream/handle/1850/11245/MNusinovThesis10-1-2009.pdf?sequence=6>>
5. McCormick, B. H.; DeFanti, T. A.; Brown, M. D. 1987. Visualization in Scientific Computing, *Computer Graphics* [interaktyvus], Volume 6, Issue 21, ACM SIGGRAPH : New York [žiūrėta 2014 m. birželio 15 d.]. Prieiga per internetą: <<http://www.evl.uic.edu/files/pdf/ViSC-1987.pdf>>
6. Bishop, M. 2003. What is computer security?, *Security & Privacy, IEEE*, Volume 1, Issue 1, p. 67–69
7. von Solms, R. 1996. Information security management: the second generation, *Computers & Security*, Volume 15, Issue 4, p. 281–8
8. *2010/2011 CSI/FBI Computer Crime and Security Survey* [interaktyvus]. 2011. Computer Security Institute, San Francisco, CA, 1 p. [žiūrėta 2016 m. vasario 4 d.]. Prieiga per internetą: <<http://gatton.uky.edu/faculty/payne/acc324/CSISurvey2010.pdf>>
9. *Key findings from the 2013 US State of Cybercrime Survey* [interaktyvus]. 2013. PwC, 6 p. [žiūrėta 2016 m. vasario 5 d.]. Prieiga per internetą: <<http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/us-state-of-cybercrime.pdf>>

10. *State of Cybersecurity: Implications for 2015* [interaktyvus]. 2015. RSA Conference & ISACA, 6 p. [žiūrėta 2016 m. vasario 5 d.]. Prieiga per internetą: <http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf>
11. von Solms, B.; von Solms, R. 2004. The 10 deadly sins of information security management, *Computers & Security*, Volume 23 Issue 5, p. 371–376
12. Sanderson, E.; Forcht, K. A. 1996. Information security in business environment, *Information Management & Computer Security*, Volume 4, Issue 1, p. 32–37
13. Ramanauskaitė, S.; Olifer, D.; Goranin, N.; Čenys, A.; Radvilavičius, L. 2014. Visualization of mapped security standards for analysis and use optimisation, *International journal of computer theory and engineering* [interaktyvus], Volume 6, Issue 5, Singapore : IACSIT Press, ISSN 1793-8201. p. 372–376 [žiūrėta 2014 m. birželio 15 d.]. Prieiga per internetą: <<http://www.ijcte.org/papers/892-S028.pdf>>
14. Telea, A.; Ersoy, O. 2010. Image-based edge bundles: Simplified visualization of large graphs, *Computer Graphics forum* [interaktyvus], Volume 29, Issue 3, Blackwell Publishing Ltd., p. 843–852 [žiūrėta 2014 m. birželio 16 d.]. Prieiga per internetą: <<http://www.rug.nl/research/portal/files/2580924/2010CompGraphForumTelea.pdf>>
15. *Know your network with LYNXeon* [interaktyvus]. 2014. 21CT, Inc. [žiūrėta 2014 m. birželio 16 d.]. Prieiga per internetą: <http://www.21ct.com/default/assets/File/WP0001_04-know-your-network-with-lynxeon.pdf>
16. *CiscoWorks Security Information Management Solution* [interaktyvus]. 2006. Cisco Systems, Inc. [žiūrėta 2014 m. birželio 17 d.]. Prieiga per internetą: <http://www.cisco.com/c/en/us/products/collateral/security/ciscoworks-security-information-management-solution/prod_white_paper0900aecd802c1c63.pdf>
17. Sandström, F. A. 2014. A test of attack graph-based evaluation of IT-security, in F.A. Sandström Master's thesis, *Umeå University, Faculty of Science and Technology, Department of Computing Science* [interaktyvus], Umeå, Sweden 9 p. [žiūrėta 2016 m. sausio 1 d.]. Prieiga per internetą: <<http://www8.cs.umu.se/education/examina/Rapporter/FredrikSandstrom.pdf>>
18. Fenton, N.; Neil, M. 2014. Decision Support Software for Probabilistic Risk Assessment using Bayesian Networks, *IEEE Software* [interaktyvus], Volume 31, Issue 2, 21 p. [žiūrėta 2016 m. sausio 1 d.]. Prieiga per internetą: <https://www.eecs.qmul.ac.uk/~norman/papers/IEEE_Prob_Risk_Assess.pdf>

19. Svensson, C. 2015. Threat modelling of historical attacks with CySeMoL, in C. Svensson Master's thesis, *KTH, School of Computer Science and Communication (CSC)* [interaktyvus], Stockholm, Sweden , p. 5–6 [žiūrėta 2016 m. sausio 2 d.]. Prieiga per internetą: < <http://www.diva-portal.org/smash/get/diva2:838530/FULLTEXT01.pdf> >
20. *A Manual for the Cyber Security Modeling Language* [interaktyvus]. 2016. Department of Industrial Information and Control Systems, Royal Institute of Technology, Stockholm, Sweden [žiūrėta 2016 m. sausio 2 d.]. Prieiga per internetą: < https://www.kth.se/ees/omskolan/organisation/avdelningar/ics/research/cc/cysemol/downloads-1_432383 >
21. Cooke, R. M. 2013. Validating Expert Judgment with the Classical Model, *Experts and Consensus in Social Science* [interaktyvus], Volume 50, Springer International Publishing, p. 191–212 [žiūrėta 2016 m. sausio 2 d.]. Prieiga per internetą: < <http://www.expertsinuncertainty.net/LinkClick.aspx?fileticket=HlcTmEoDunY%3D&tabid=4385&mid=8296> >
22. *The Cyber Security Modeling Language (CySeMoL)* [interaktyvus]. 2016. Department of Industrial Information and Control Systems, Royal Institute of Technology, Stockholm, Sweden [žiūrėta 2016 m. sausio 2 d.]. Prieiga per internetą: < <http://www.kth.se/en/ees/omskolan/organisation/avdelningar/ics/research/cc/cysemol> >
23. *Tutorial: Introduction to Flash* [interaktyvus]. 2014. The Regents of the University of California [žiūrėta 2015 m. sausio 14 d.]. Prieiga per internetą: < <http://multimedia.journalism.berkeley.edu/tutorials/introduction-to-flash/> >
24. *Adobe Flash Player 9 Security* [interaktyvus]. 2008. Adobe Systems Incorporate [žiūrėta 2015 m. sausio 14 d.]. Prieiga per internetą: < <http://citeserx.ist.psu.edu/viewdoc/download;jsessionid=EC47A3765E9A18C7E99652C769F7D1AB?doi=10.1.1.304.8724&rep=rep1&type=pdf> >
25. *Canvas API* [interaktyvus]. 2015. Mozilla Developer Network and individual contributors [žiūrėta 2015 m. sausio 15 d.]. Prieiga per internetą: < https://developer.mozilla.org/en-US/docs/Web/API/Canvas_API >
26. *HTML Canvas 2D Context* [interaktyvus]. 2015. W3C [žiūrėta 2015 m. sausio 15 d.]. Prieiga per internetą: < <http://www.w3.org/TR/2dcontext/> >
27. *Scalable Vector Graphics 2* [interaktyvus]. 2015. W3C [žiūrėta 2015 m. sausio 16 d.]. Prieiga per internetą: < <http://www.w3.org/TR/SVG2/intro.html> >

28. *HTML & CSS* [interaktyvus]. 2015. W3C [žiūrėta 2015 m. sausio 16 d.]. Prieiga per internetą: < <http://www.w3.org/standards/webdesign/htmlcss> >
29. Kallem, A. 2010. Visualization for Verification Driven Learning in Database Studies, *University of New Orleans Theses and Dissertations* [interaktyvus], p. 6–7 [žiūrėta 2015 m. sausio 17 d.]. Prieiga per internetą: < <http://scholarworks.uno.edu/cgi/viewcontent.cgi?article=1098&context=td> >
30. *WebGL* [interaktyvus]. 2015. Khronos Group [žiūrėta 2015 m. sausio 17 d.]. Prieiga per internetą: < <https://www.khronos.org/webgl/> >
31. Büchele, D; Ismair, S. 2013. 3D Graphics in the Browser Using WebGL, *Ludwig Maximilian University of Munich* [interaktyvus], p. 1–3 [žiūrėta 2015 m. sausio 17 d.]. Prieiga per internetą: < <http://static1.squarespace.com/static/5068960be4b01308d46e1e9c/t/50fea3fbe4b0499abb09eab9/1358865403954/spwal.pdf> >
32. *WebGL Security* [interaktyvus]. 2015. Khronos Group [žiūrėta 2015 m. sausio 17 d.]. Prieiga per internetą: < <https://www.khronos.org/webgl/security/> >
33. *WebGL – More WebGL Security Flaws* [interaktyvus]. 2011. Context Information Security [žiūrėta 2015 m. sausio 17 d.]. Prieiga per internetą: < <http://www.contextis.com/resources/blog/webgl-more-webgl-security-flaws/> >
34. *Risk Management Guide for Information Technology Systems* [interaktyvus]. 2002. NIST Special Publication 800-30 [žiūrėta 2016 m. vasario 25 d.]. Prieiga per internetą: < <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf> >
35. Sandhu, R. S. 1998. Role-based Access Control, *Advances in Computers* [interaktyvus], Volume 46, Academic Press, p. 237–286 [žiūrėta 2016 m. kovo 5 d.]. Prieiga per internetą: < http://profsandhu.com/articles/advcom/adv_comp_rbac.pdf >
36. Joshi, J. B. D.; Aref, W. G.; Ghafoor, A.; Spafford, E. H. 2001. Security models for web-based applications, *Communications of the ACM* [interaktyvus], Volume 44, Issue 2, ACM, New York, USA, p. 38–44 [žiūrėta 2016 m. kovo 5 d.]. Prieiga per internetą: < http://www.sis.pitt.edu/jjoshi/WebModels_CACM01.pdf >
37. *HTML Color Names* [interaktyvus]. 2015. Refsnes Data [žiūrėta 2015 m. kovo 10 d.]. Prieiga per internetą: < http://www.w3schools.com/colors/colors_names.asp >
38. Benedetto, M. D.; Ponchio, F.; Ganovelli, F.; Scopigno, R. 2010. SpiderGL: A JavaScript 3D Graphics Library for Next-Generation WWW, in *Proc. of the 15th International*

Conference on Web 3D Technology, ACM, New York, NY, USA, 2010 [interaktyvus].

Web3D '10, p. 165–174 [žiūrėta 2015 m. kovo 12 d.]. Prieiga per internetą: <

<http://vcg.isti.cnr.it/Publications/2010/DPGS10/spidergl.pdf> >

39. Tamal, D. 2011. Acomparative Analysis on Modeling and Implementing with MVC Architecture, in *IJCA Proc. on International Conference on Web Services Computing (ICWSC), 2011* [interaktyvus]. p. 44–49 [žiūrėta 2015 m. kovo 15 d.]. Prieiga per internetą: < <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.472.1591&rep=rep1&type=pdf> >

40. TreeJS [interaktyvus] 2014. [žiūrėta 2014 m. birželio 18 d.]. Prieiga per internetą: < <http://threejs.org/> >

Priedai

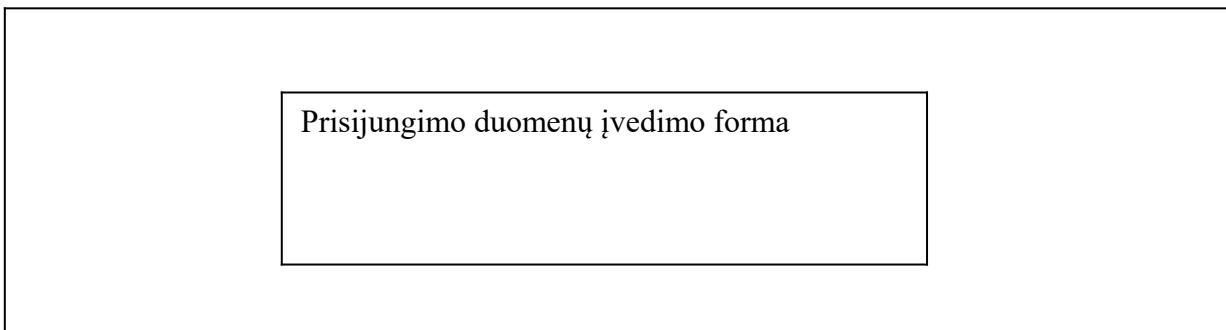
A priedas. Grafinė vartotojo sąsaja

B priedas. Langų maketai ir piktogramos

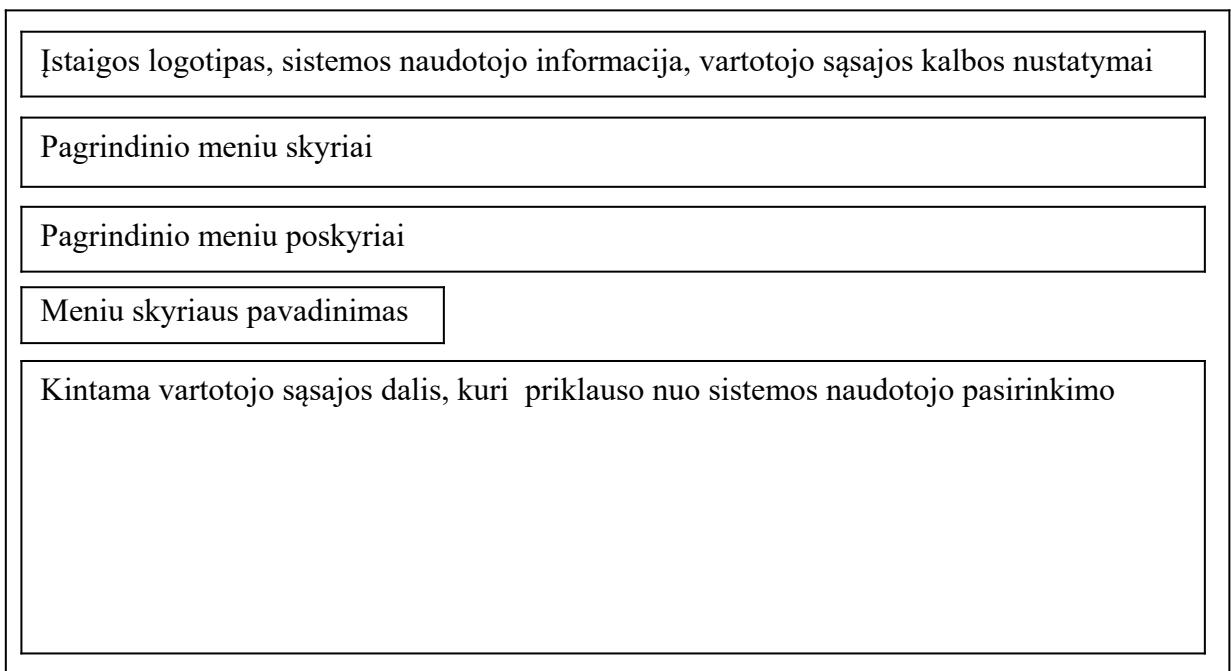
C priedas. Užduočių formulavimo būdo reikalavimų dalis

A Priedas. Grafinė vartotojo sasaja

GVSR-1 Grafinė vartotojo sasaja prisijungimams prie sistemos.



GVSR-2 Grafinė vartotojo sasaja sėkmingai prisijungus prie sistemos.



B Priedas. Langų maketai ir piktogramos

1. Langų maketai

Grafinės vartotojo sąsajos GVSR-2 kintamosios dalies langų maketai pateikti 1.1. ir 1.2. skirsniuose.

1.1. Informacijos sąrašų langai

ID	Lango maketas	
<u>ULMSR-1</u>	Puslapiavimo nustatymas ir mygtukai	Veiksmų mygtukai
	Vieta informacijos sąrašui	Piktogramų sąrašas
	Puslapiavimo nustatymas ir mygtukai	Veiksmų mygtukai
<u>ULMSR-2</u>	Puslapiavimo nustatymas ir mygtukai	
	Iššokanti klaidos pranešimo vieta	
	Vieta duomenų įvedimui	Veiksmų mygtukai
	Vieta informacijos sąrašui	Piktogramų sąrašas
	Puslapiavimo nustatymas ir mygtukai	
<u>ULMSR-3</u>	Puslapiavimo nustatymas ir mygtukai	Veiksmų mygtukai
	Vieta paieškos organizavimui ir duomenų filtravimui	
	Iššokanti duomenų įvedimo vieta	
	Vieta informacijos sąrašui	Piktogramų sąrašas
	Galimi pateiktos informacijos detalizavimo sąrašai	
<u>ULMSR-4</u>	Puslapiavimo nustatymas ir mygtukai	Veiksmų mygtukai
	Veiksmų mygtukai	Sąrašo filtravimo laukas
	Vieta informacijos sąrašui	Puslapiavimo mygtukai
	Piktogramų sąrašas	Veiksmų mygtukai
	Veiksmų mygtukai	Vieta informacijos sąrašui
		Piktogramų sąrašas
		Puslapiavimo mygtukai
		Veiksmų mygtukai

<u>ULMSR-5</u>	<table border="1"> <tr> <td>Sąrašo filtravimo laukas</td> <td></td> </tr> <tr> <td>Puslapiavimo nustatymas ir mygtukai</td><td>Veiksmų mygtukai</td> </tr> <tr> <td>Vieta informacijos sąrašui</td><td>Piktogramų sąrašas</td> </tr> <tr> <td>Puslapiavimo nustatymas ir mygtukai</td><td>Veiksmų mygtukai</td> </tr> </table>	Sąrašo filtravimo laukas		Puslapiavimo nustatymas ir mygtukai	Veiksmų mygtukai	Vieta informacijos sąrašui	Piktogramų sąrašas	Puslapiavimo nustatymas ir mygtukai	Veiksmų mygtukai						
Sąrašo filtravimo laukas															
Puslapiavimo nustatymas ir mygtukai	Veiksmų mygtukai														
Vieta informacijos sąrašui	Piktogramų sąrašas														
Puslapiavimo nustatymas ir mygtukai	Veiksmų mygtukai														
<u>ULMSR-6</u>	<table border="1"> <tr> <td>Sąrašo filtravimo laukas</td> <td></td> </tr> <tr> <td>Priskyrimo būdo pasirinkimas</td><td></td> </tr> <tr> <td>Puslapiavimo nustatymas ir mygtukai</td><td>Veiksmų mygtukai</td> </tr> <tr> <td>Vieta informacijos sąrašui</td><td>Vieta priskyrimo sąrašams</td> </tr> <tr> <td>Puslapiavimo nustatymas ir mygtukai</td><td>Veiksmų mygtukai</td> </tr> </table>	Sąrašo filtravimo laukas		Priskyrimo būdo pasirinkimas		Puslapiavimo nustatymas ir mygtukai	Veiksmų mygtukai	Vieta informacijos sąrašui	Vieta priskyrimo sąrašams	Puslapiavimo nustatymas ir mygtukai	Veiksmų mygtukai				
Sąrašo filtravimo laukas															
Priskyrimo būdo pasirinkimas															
Puslapiavimo nustatymas ir mygtukai	Veiksmų mygtukai														
Vieta informacijos sąrašui	Vieta priskyrimo sąrašams														
Puslapiavimo nustatymas ir mygtukai	Veiksmų mygtukai														
<u>ULMSR-7</u>	<table border="1"> <tr> <td>Sistemos pranešimas</td> <td></td> </tr> <tr> <td>Rizikos matrica</td><td>Veiksmų mygtukai</td> </tr> <tr> <td>Tikimybės laipsnių sąrašas</td><td>Piktogramų sąrašas</td> </tr> <tr> <td>Poveikio laipsnių sąrašas</td><td>Piktogramų sąrašas</td> </tr> <tr> <td>Rizikos laipsnių sąrašas</td><td>Spalvos nustatymas</td> </tr> <tr> <td></td><td>Piktogramų sąrašas</td> </tr> <tr> <td></td><td>Veiksmų mygtukai</td> </tr> </table>	Sistemos pranešimas		Rizikos matrica	Veiksmų mygtukai	Tikimybės laipsnių sąrašas	Piktogramų sąrašas	Poveikio laipsnių sąrašas	Piktogramų sąrašas	Rizikos laipsnių sąrašas	Spalvos nustatymas		Piktogramų sąrašas		Veiksmų mygtukai
Sistemos pranešimas															
Rizikos matrica	Veiksmų mygtukai														
Tikimybės laipsnių sąrašas	Piktogramų sąrašas														
Poveikio laipsnių sąrašas	Piktogramų sąrašas														
Rizikos laipsnių sąrašas	Spalvos nustatymas														
	Piktogramų sąrašas														
	Veiksmų mygtukai														
<u>ULMSR-8</u>	<table border="1"> <tr> <td>Puslapiavimo nustatymas ir mygtukai</td> <td></td> </tr> <tr> <td>Iššokanti klaidos pranešimo vieta</td><td></td> </tr> <tr> <td>Rizikos matrica</td><td></td> </tr> <tr> <td>Naujo rizikos valdymo ataskaitos inicijavimo forma</td><td>Veiksmų mygtukai</td> </tr> <tr> <td>Vieta informacijos sąrašui</td><td>Trynimo piktograma, peržiūros mygtukas, ir pasirinkimo laukai</td> </tr> <tr> <td>Puslapiavimo nustatymas ir mygtukai</td><td>Veiksmų mygtukai</td> </tr> </table>	Puslapiavimo nustatymas ir mygtukai		Iššokanti klaidos pranešimo vieta		Rizikos matrica		Naujo rizikos valdymo ataskaitos inicijavimo forma	Veiksmų mygtukai	Vieta informacijos sąrašui	Trynimo piktograma, peržiūros mygtukas, ir pasirinkimo laukai	Puslapiavimo nustatymas ir mygtukai	Veiksmų mygtukai		
Puslapiavimo nustatymas ir mygtukai															
Iššokanti klaidos pranešimo vieta															
Rizikos matrica															
Naujo rizikos valdymo ataskaitos inicijavimo forma	Veiksmų mygtukai														
Vieta informacijos sąrašui	Trynimo piktograma, peržiūros mygtukas, ir pasirinkimo laukai														
Puslapiavimo nustatymas ir mygtukai	Veiksmų mygtukai														
<u>ULMSR-9</u>	<table border="1"> <tr> <td>Puslapiavimo nustatymas ir mygtukai</td> <td>Veiksmų mygtukai</td> </tr> <tr> <td>Grįžimo atgal mygtukas</td><td>Rizikos valdymo dalies pasirinkimas</td> </tr> <tr> <td>Vieta informacijos sąrašui</td><td>Užpildyti duomenų formą</td> </tr> <tr> <td>Puslapiavimo nustatymas ir mygtukai</td><td>Veiksmų mygtukai</td> </tr> </table>	Puslapiavimo nustatymas ir mygtukai	Veiksmų mygtukai	Grįžimo atgal mygtukas	Rizikos valdymo dalies pasirinkimas	Vieta informacijos sąrašui	Užpildyti duomenų formą	Puslapiavimo nustatymas ir mygtukai	Veiksmų mygtukai						
Puslapiavimo nustatymas ir mygtukai	Veiksmų mygtukai														
Grįžimo atgal mygtukas	Rizikos valdymo dalies pasirinkimas														
Vieta informacijos sąrašui	Užpildyti duomenų formą														
Puslapiavimo nustatymas ir mygtukai	Veiksmų mygtukai														

<u>ULMSR-10</u>	<p>Naujo objekto sukūrimo forma</p> <p>Puslapiavimo nustatymas ir mygtukai</p> <p>Iššokanti klaidos pranešimo vieta</p> <p>Objekto duomenys ir panaikinimo piktograma</p> <p>Vertybės ir jos formos duomenys, ir formos panaikinimo piktograma</p> <p>Puslapiavimo nustatymas ir mygtukai</p>	<p>Objekto pasirinkimas ir matmenų nustatymo forma</p> <p>Vertybų vizualizacija objekte</p> <p>Veiksmų mygtukai</p>
<u>ULMSR-11</u>	<p>Rizikos matrica</p> <p>Objekto ir ataskaitos pasirinkimo forma</p> <p>Iššokanti klaidos pranešimo vieta</p> <p>Objektui kylančių rizikų sąrašas</p> <p>Rizikos apskaičiavimo duomenys</p>	<p>Veiksmų mygtukai</p> <p>Objekte kylančių grėsmių ir rizikos vizualizacija</p>
<u>ULMSR-12</u>	<p>Puslapiavimo nustatymas ir mygtukai</p> <p>Grįžimo atgal mygtukas</p> <p>Rodyklė</p> <p>Vieta informacijos sąrašui</p> <p>Puslapiavimo nustatymas ir mygtukai</p>	<p>Pokyčių piktogramos ir rizikos laipsniai</p>

1.2. Duomenų įvedimo langas

Gryžimo atgal mygtukas	ID Iššokanti klaidos pranešimo vieta	Lango maketas	Veiksmų mygtukai
	<u>ULMDR-1</u>		

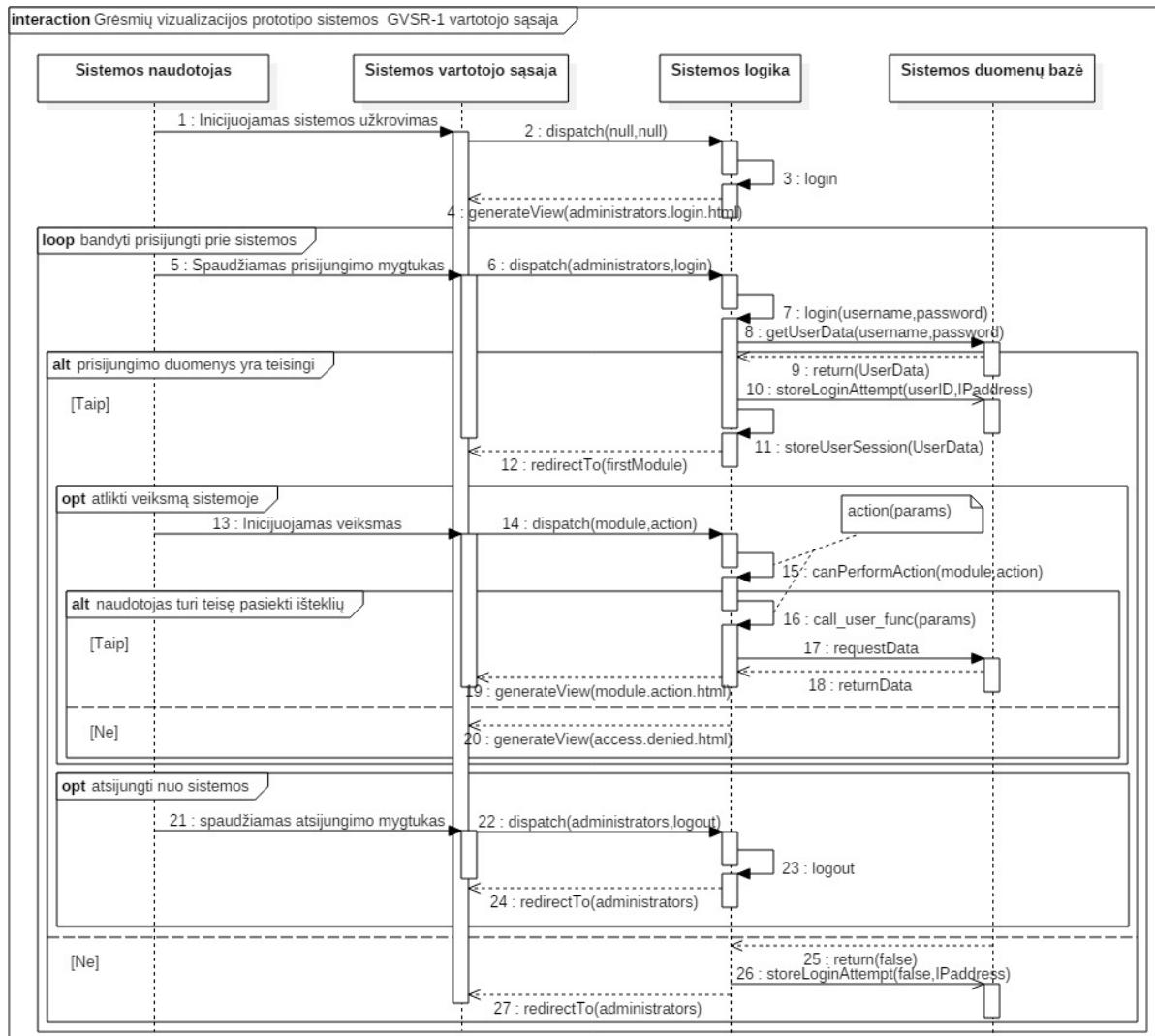
2. Piktogramos

14 lentelė. Piktogramų sąrašas

ID	Piktogra-ma	Reikšmė
UPR-1		Naujame lange inicijuoti įrašo duomenų peržiūrą.
UPR-2		Naujame lange inicijuoti įrašo duomenų keitimą.
UPR-3		Tame pačiame lange inicijuoti įrašo duomenų ištrynimą.
UPR-4		Tame pačiame lange suformuoti naują laikiną slaptažodį.
UPR-5		Tame pačiame lange užpildyti laikino slaptažodžio duomenų įvedimo laukus.
UPR-6		Tame pačiame lange atvaizduoti klaidos pranešimą.
UPR-7		Inicijuoti naujo duomenų įrašo pridėjimą prie sąrašo.
UPR-8		Kitiems sistemos naudotojams šis įrašas yra atvaizduojamas.
UPR-9		Kitiems sistemos naudotojams šis įrašas yra nematomas.
UPR-10		Įspėja apie vertybės būsenos pasikeitimą iki nepriimtino lygio.
UPR-11		Aktyvuoti iššokantį kalendorių datos pasirinkimui.
UPR-12		Naujame lange inicijuoti įrašo komentavimą.
UPR-13		Tame pačiame lange inicijuoti formos duomenų ištrynimą iš vizualizacijos.
UPR-14		Atskaitos taškas rizikos valdymo ataskaitų pokyčių analizei
UPR-15		I rizikos valdymo ataskaitą įtraukta nauja rizika
UPR-16		Iš rizikos valdymo ataskaitos pašalinta rizika
UPR-17		Rizikos lygis sumažėjo
UPR-18		Rizikos lygis išliko toks pat
UPR-19		Rizikos lygis padidėjo
UPR-20		Išskleidžia vertybų ir jų rizikos laipsnių sąrašą
UPR-21		Suskleidžia vertybų ir jų rizikos laipsnių sąrašą

C Priedas. Užduočių formulavimo būdo reikalavimų dalis

UFBR-1 Pagal GVSR-1 vartotojo sąsają užduoties GVSU-1 vykdymo žingsniai atvaizduoti UML sekų diagramoje (žr. 27 pav.).



27 pav. GVSU-1 užduoties sekų diagrama

Sekų diagramoje (žr. 27 pav.) pateikti sistemos ryšiai tarp 4 sistemos elementų:

- 1 Sistemos naudotojo, kuris naudodamas kompiuterinėmis priemonėmis jungiasi prie sistemos ir naudojasi jos funkcionalumu;
- 2 Sistemos vartotojo sasajos (GVSR-1);
- 3 Sistemos loginio elemento, kuris vykdo sistemos vartotojo sasajoje sistemos naudotojo inicijuotus veiksmus;

4 Sistemos duomenų bazės, kurioje saugomi sistemos duomenys, kurie yra formuojami pagal sistemos logikos funkcionalumą.

Sekų diagramoje (žr. 27 pav.) pateikti sistemos elementų tarpusavio sąveikos žingsniai:

1 pirmą kartą jungiantis sistemos naudotojas interneto naršyklės adreso lange iniciuoja prisijungimą prie sistemos patvirtindamas įvestą sistemos adresą;

2–3 pirmą kartą jungiantis sistemos naudotojas nukreipiamas vykdyti sistemos *login* komandą;

4 sistemos naudotojui pateikiama prisijungimo prie sistemos vartotojo sasaja GVSR-1;

5 kiekvieną kartą bandant jungtis prie sistemos įvedami prisijungimo duomenys ir spaudžiamas prisijungimo mygtukas;

6–7 sistema apdoroja sistemos naudotojo įvestus duomenis *login* komanda ir formuoja kreipimąsi į duomenų bazę;

8 sistemos duomenų bazė grąžina paieškos rezultatus;

9–10 jeigu sistemos duomenų bazė grąžina sistemos naudotojo duomenis, tada duomenų bazėje išsaugojamas sistemos naudotojo prisijungimo prie sistemos žurnalinis įrašas;

11–12 sistemos naudotojui sistemoje sukuriama sesija tolesniams darbo organizavimui ir vykdomas sistemos vartotojo sasajos nukreipiamas į pirmąjį sistemos išteklių GVSR-2 vartotojo sasajoje, kurį sistemos naudotojas turi teisę pasiekti (14–19 žingsniai);

13 sistemos naudotojo, prisijungusio prie sistemos, visi tolesni veiksmai gali būti apibūdinami 13–20 žingsniais. Iš pradžių iniciuojamas veiksmas;

14 sistemos naudotojas GVSR-2 vartotojo sasajoje iniciuoja tam tikro meniu skyriaus veiksmą *action*;

15–16 užprašomi sistemos techniniai ištekliai apie naudotojo turimas teises sistemoje ir tikrinama ar sistemos naudotojas gali atliliki veiksmą *action*;

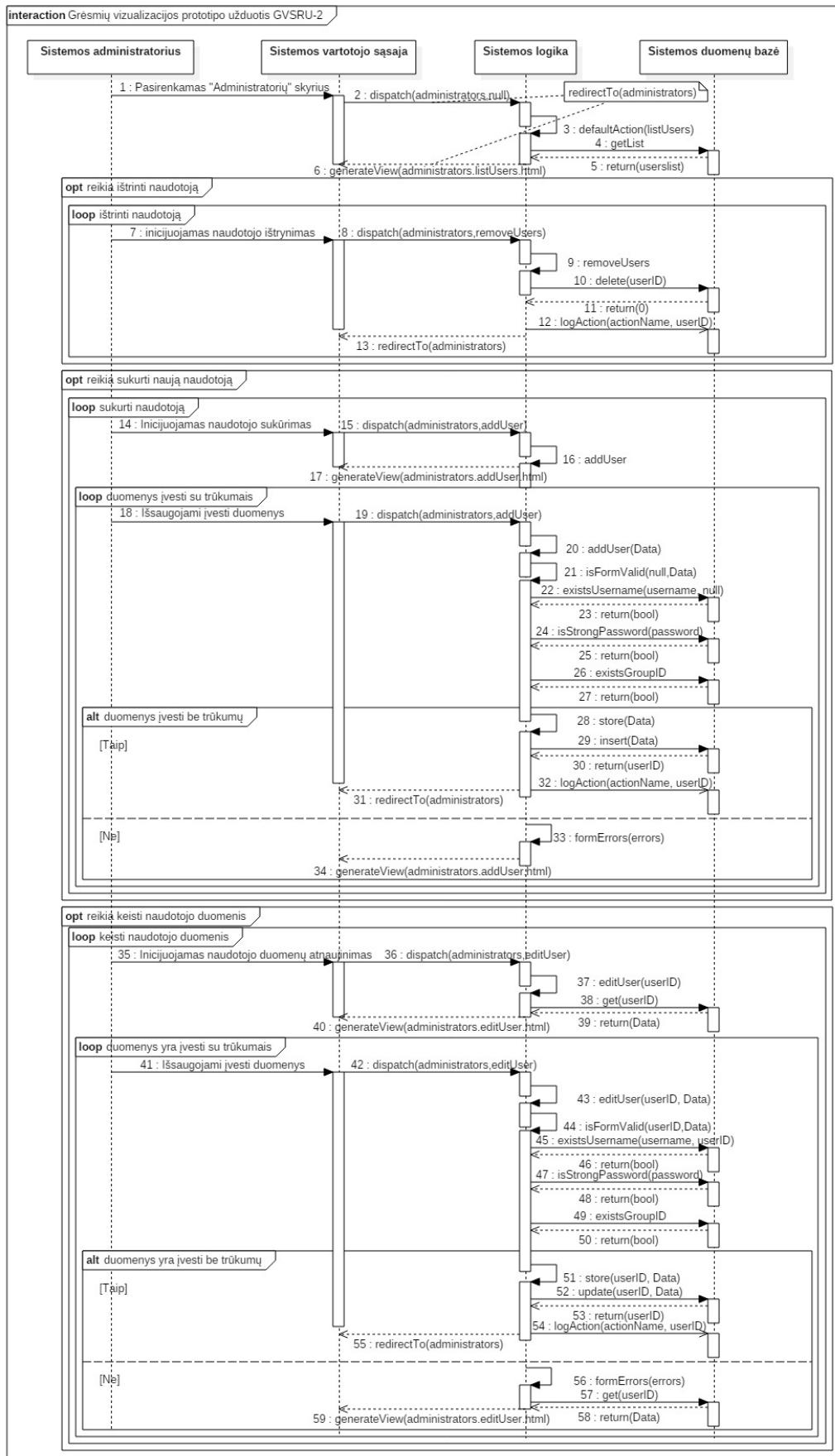
16–19 jeigu sistemos naudotojui leidžiama, įvykdomas veiksmas *action*. Šio veiksmo metu gali būti vykdomos užklausos į duomenų bazę ir gaunami duomenys, kuriuos sistema atvaizduoja vartotojo sasajoje pagal iš anksto paruoštą lango maketo šabloną;

20 jeigu sistemos naudotojui draužiama pasiekti išteklių pateikiamas tokio draudimo pranešimas;

21–24 sistemos naudotojui siekiant atsijungti iš GVSR-2 vartotojo sąsajos spaudžiamas atsijungimo mygtukas, kuris įvykdo *logout* komandą ir nukreipia sistemos naudotoją į prisijungimo prie sistemos pradžios langą (2–4 žingsniai);

25–27 jeigu sistemos duomenų bazė grąžina neigiamą rezultatą, sistema išsaugoja bandymo jungtis žurnalinį įrašą duomenų bazėje ir toliau vykdo sistemos vartotojo sąsajos nukreipimą (2–4 žingsniai) ir leidžia sistemos naudotojui pakartotinai bandyti jungtis prie sistemos nuo 5 žingsnio.

UFBR-2 Pagal GVSR-2 vartotojo sąsają užduoties GVSRU-2 vykdymo žingsniai atvaizduoti UML sekų diagramoje (žr. 28 pav.). Kaip ir UFBR-1 šioje sekų diagramoje pateikti ryšiai tarp tų pačių sistemos 4 elementų nenagrinėjant GVSR-1 vartotojo sąsajos dalies.



28 pav. GVSU-2 užduoties sekų diagrama

Sekų diagramoje (žr. 28 pav.) pateikti sistemos elementų tarpusavio sąveikos žingsniai, kuriuos vykdo sistemos administratorius siekdamas atlkti sistemos naudotojų administravimą:

1–6 sistemos administratoriui pasirinkus meniu skyrių „Administratoriai“ sistema pateikia sistemos naudotojų sąrašą pagal GVSRU-2 *listUsers* komanda suformuotą ULMSR-1 langą;

7–13 sistemos administratorius siekiantis ištrinti neberekalingą sistemos naudotoją ULMSR-1 lange pateiktame sistemos naudotojų sąraše spaudžia pasirinkto naudotojo juosteje esančią UPR-3 piktogramą. Sistema įvykdo komandą *removeUser* ir ištrina pasirinktą sistemos naudotoją (nėra galimybės ištrinti sistemos naudotoją su sistemos administratoriaus teisėmis) ir sistemos administratorius nukreipiamas į sistemos naudotojų sąrašą (2–6 žingsniai). Šiuos žingsnius sistemos administratorius kartoja tiek kartą, kiek reikia ištrinti sistemos naudotojų;

14–17 sistemos administratorius siekiantis sukurti naują sistemos naudotojo įrašą ULMSR-1 lango veiksmų juosteje spaudžia mygtuką „Sukurti“, kuris sistemoje iniciuoja komandą *addUser* ir vartotojo sąsajoje atvaizduoja ULMDR-1 langą;

18–27 sistemos administratorius įveda formos duomenis ir spaudžia ULMDR-1 veiksmų juosteje esantį duomenų išsaugojimo mygtuką, tada sistemoje pakartotinai iniciuojamas *addUser* komandos vykdymas;

28–31 jeigu duomenys yra įvesti taisyklingai, tada nauji sistemos naudotojo duomenys įvedami į duomenų bazę ir sistemos administratorius nukreipiamas į sistemos naudotojų sąrašą (2–6 žingsniai);

33–34 jeigu duomenys yra įvesti netaisyklingai ULMDR-1 klaidos pranešimo vietoje atvaizduoja pranešimą apie įvykusią klaidą ir kartojamas žingsnis nuo 18;

35–40 sistemos administratorius siekiantis keisti sistemos naudotojo duomenis ULMSR-1 lange pasirinkto sistemos naudotojo juosteje spaudžia UPR-2 piktogramą, kuri įvykdo *editUser* komandą ir pateikia ULMDR-1 duomenų įvesties langą;

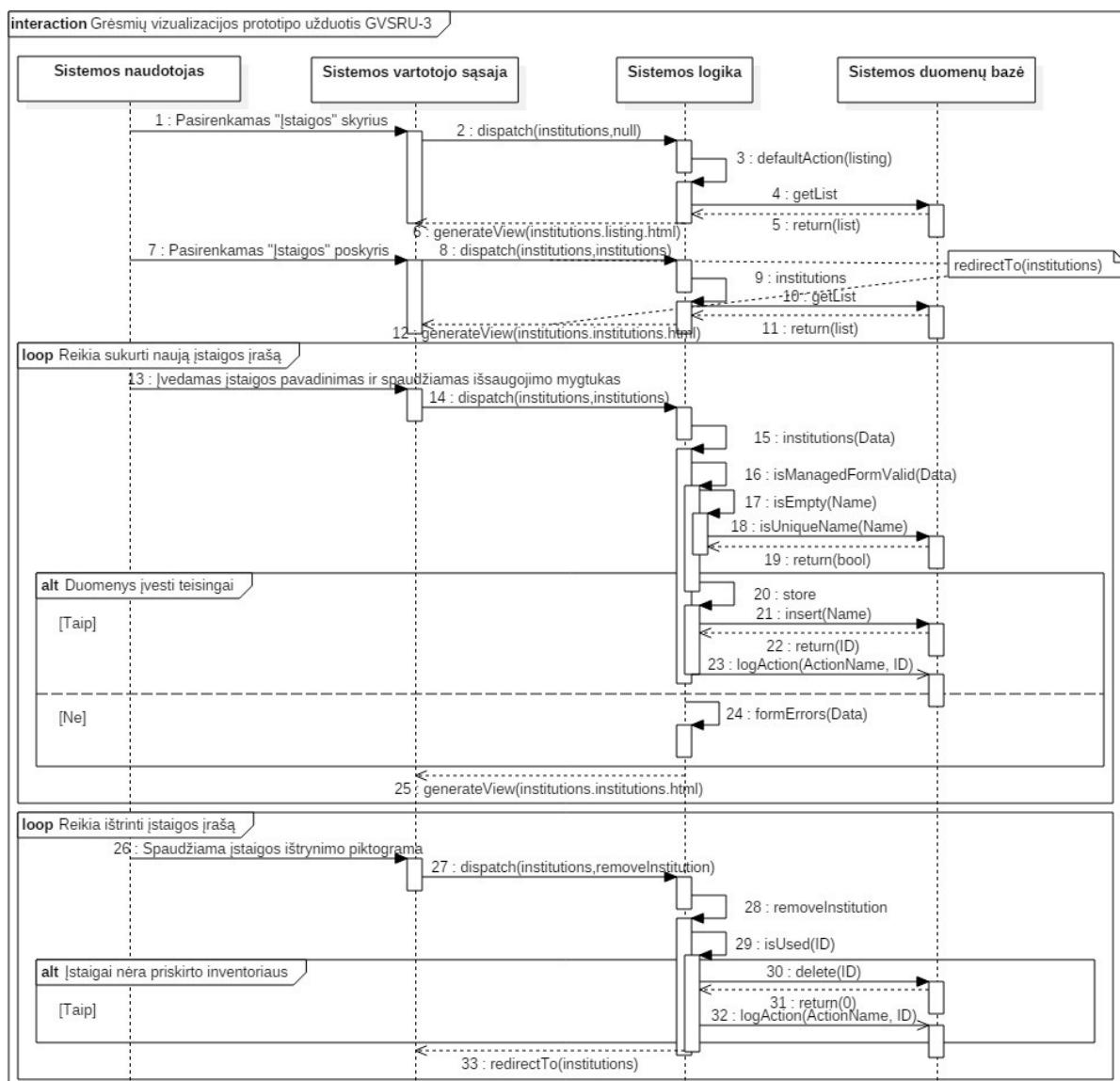
41–50 sistemos administratorius pakeičia sistemos naudotojo duomenis ir spaudžia ULMDR-1 veiksmų juosteje esantį duomenų išsaugojimo mygtuką. Vykdoma *editUser* komanda bei apdorojami formoje įvesti ar pakeisti duomenys;

51–55 jeigu įvesti duomenys atitinka sistemos reikalavimus (tokio sistemos naudotojo prisijungimo vardo sistemos duomenų bazėje nėra, įvestas pakankamo ilgio slaptažodis, teisingai pasirinktas sistemos naudotojo grupės identifikacinis numeris ir kita), tada vykdomas sistemos naudotojo duomenų atnaujinimas. Lygiagrečiai išsaugojamas žurnalinis įrašas apie

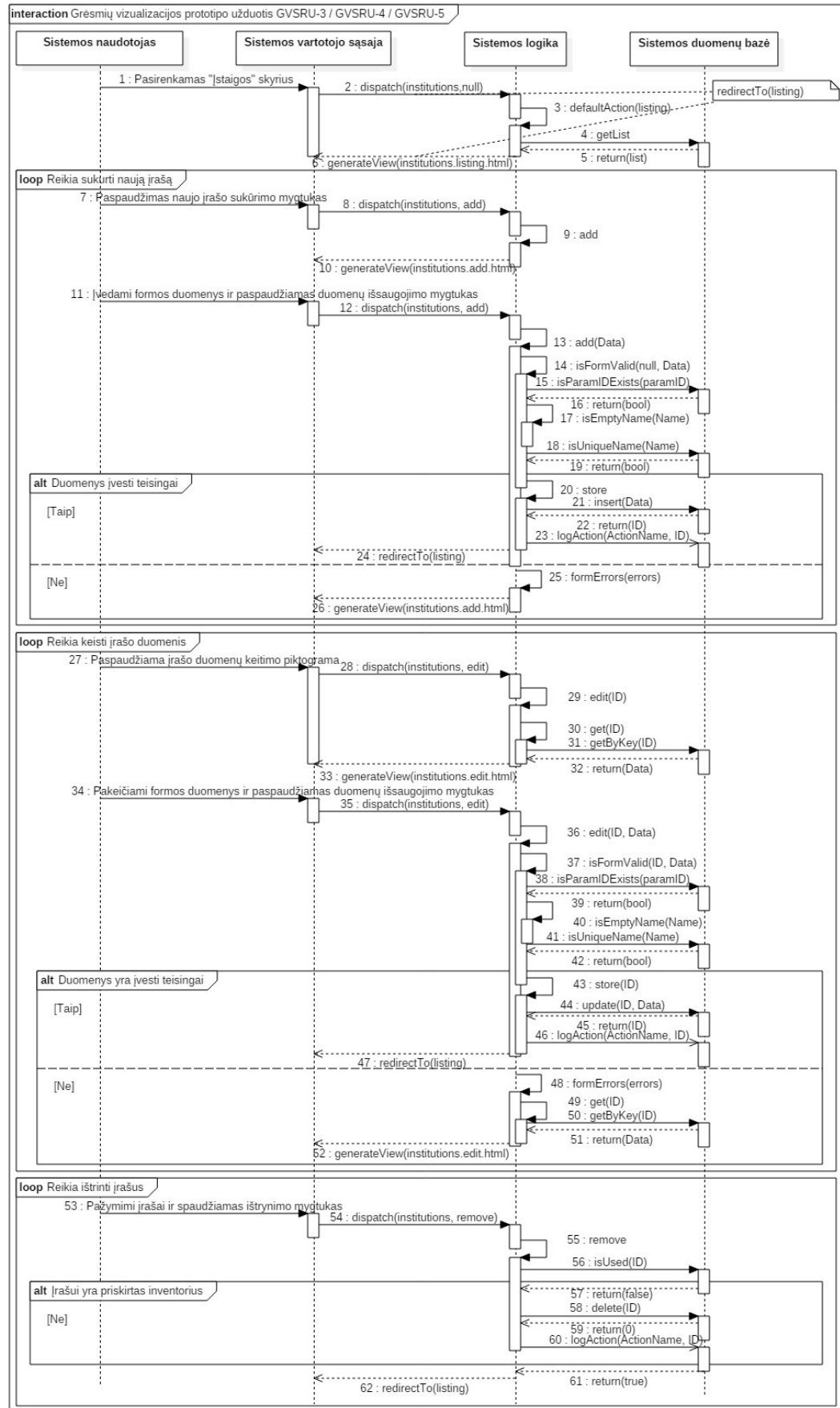
sistemos administratoriaus atliktą veiksmą ir vykdomas vartotojo sėsajos nukreipimas į sistemos naudotojų sąrašą (2–6 žingsniai);

56–59 jeigu duomenys yra įvesti netaisyklingai ULMDR-1 klaidos pranešimo vietoje atvaizduoja pranešimą apie įvykusią klaidą ir kartoamas žingsnis nuo 41.

UFBR-3 Pagal GVSR-2 vartotojo sėsają užduoties GVSRU-3 vykdymo žingsniai atvaizduoti UML sekų diagramose (žr. 29 ir 30 pav.). Kaip ir UFBR-1 šioje sekų diagramoje pateikti ryšiai tarp tų pačių sistemos 4 elementų nenagrinėjant GVSR-1 vartotojo sėsajos dalies.



29 pav. GVSRU-3 užduoties sekų diagramos dalis



30 pav. GVSU-3, GVSU-4, GVSU-5 užduočių sekų diagramos dalis

Sekų diagramoje (žr. 29 pav.) pateikti sistemos elementų tarpusavio sąveikos žingsniai, kuriuos vykdo vertybų priežiūros grupės narys siekdamas apibrėžti administruojamą įstaigą sąrašą:

1–6 vertybų priežiūros grupės nariui pasirinkus meniu skyrių „Įstaigos“ sistema pateikia įstaigų struktūrinius duomenis pagal GVSRU-3 *listing* komanda suformuotą ULMSR-1 langą;

7–12 vertybų priežiūros grupės nariui pasirinkus „Įstaigos“ meniu skyriaus „Įstaigos“ poskyrį sistema pateikia įstaigų sąrašo duomenis pagal GVSRU-3 *institutions* komanda suformuotą ULMSR-2 langą;

13–19 vertybų priežiūros grupės narys siekiantis sukurti naują įstaigos įrašą įveda įstaigos pavadinimą į tam skirtą formos vietą ir spaudžia ULMSR-2 išsaugojimo veiksmų mygtuką, kuris iniciuoja įvestų duomenų patikrimimą komanda *institutions*;

20–23 jeigu duomenys yra įvesti taisyklingai (formos laukas nėra tuščias ir pavadinimas yra unikalus, ir nesikartoja), tada jie išsaugojami sistemos duomenų bazėje kartu su atlikto veiksmo žyma;

24 jeigu duomenys yra įvesti netaisyklingai sistema formuoja klaidos pranešimą;

25 vertybų priežiūros grupės nariui ULMSR-2 lange pateikiami įstaigų sąrašo duomenys ir klaidos pranešimas, jeigu klaidingai buvo vedami įstaigos duomenys;

26–29 vertybų priežiūros grupės narys siekiantis ištinti įstaigos įrašą ULMSR-2 lange spaudžia UPR-3 įstaigos ištrynimo piktogramą. Sistema pradeda vykdyti *removeInstitution* komandą ir atlieka tikrinimą ar pasirinkta įstaiga turi priskirtų vertybų;

30–32 jeigu įstaigoje nėra priskirtų vertybų, tada ištrinamas įstaigos įrašas, duomenų bazėje išsaugojama atlikto veiksmo žymė;

33 vertybų priežiūros grupės narj sistema nukreipia į „Įstaigos“ meniu skyriaus „Įstaigos“ poskyrį (7–12 žingsniai).

Sekų diagramoje (žr. 30 pav.) pateikti sistemos elementų tarpusavio sąveikos žingsniai, kuriuos vykdo vertybų priežiūros grupės narys siekdamas apibrėžti įstaigos struktūrą ir disponuojamas vertybės:

1–6 vertybų priežiūros grupės nariui pasirinkus meniu skyrių „Įstaigos“ sistema pateikia įstaigų struktūrinius duomenis pagal GVSRU-3 *listing* komanda suformuotą ULMSR-1 langą;

7–10 vertybių priežiūros grupės narys siekiantis sukurti naują struktūrinio padalinio įrašą spaudžia mygtuką „Sukurti“ ir inicijuoja *add* komandos vykdymą, sistema pateikia ULMDR-1 duomenų įvesties langą;

11–19 vertybių priežiūros grupės narys įvedės formos duomenis spaudžia ULMDR-1 veiksmų juostoje esantį duomenų išsaugojimo mygtuką, tada sistemoje pakartotinai inicijuojamas *add* komandos vykdymas, tikrinami įvesti duomenys (įvesti atitinkami formos laukai yra netušti, unikalūs ir nepasikartojantys, pasirenkamas tinkamas įstaigos identifikacinis numeris);

20–24 jeigu duomenys yra įvesti taisyklingai, tada sistema išsaugoja struktūrinio padalinio duomenų įrašą kartu su atlikto veiksmo žyme duomenų bazėje ir nukreipia vertybių priežiūros grupės narį į įstaigos struktūrinių duomenų sąrašą (2–6 žingsniai);

25–26 jeigu įvedamai duomenys netaisyklingai ULMDR-1 klaidos pranešimo vietoje atvaizduoja pranešimą apie įvykusią klaidą ir kartojamas žingsnis nuo 11;

27–33 vertybių priežiūros grupės narys siekiantis keisti struktūrinio padalinio duomenis ULMSR-1 lange pasirinkto padalinio juostoje spaudžia UPR-2 piktogramą, kuri įvykdo *edit* komandą ir pateikia ULMDR-1 duomenų įvesties langą;

34–42 vertybių priežiūros grupės narys pakeičia struktūrinio padalinio duomenis ir spaudžia ULMDR-1 veiksmų juostoje esantį duomenų išsaugojimo mygtuką. Vykdoma *edit* komanda bei apdorojami formoje įvesti ar pakeisti duomenys;

43–47 jeigu įvesti duomenys atitinka sistemos reikalavimus (įvesti atitinkami formos laukai yra netušti, unikalūs ir nepasikartojantys, pasirenkamas tinkamas įstaigos identifikacinis numeris), tada vykdomas struktūrinio padalinio duomenų atnaujinimas. Lygiagrečiai išsaugojamas žurnalinis įrašas apie vertybių priežiūros grupės nario atliktą veiksmą ir vykdomas vartotojo sąsajos nukreipimas į įstaigos struktūrinių duomenų sąrašą (2–6 žingsniai);

48–52 jeigu duomenys yra įvesti netaisyklingai ULMDR-1 klaidos pranešimo vietoje sistema atvaizduoja pranešimą apie įvykusią klaidą ir kartojamas žingsnis nuo 34;

53–62 vertybių priežiūros grupės narys siekiantis ištrinti neberekalingą struktūrinį padalinį ULMSR-1 lange pateiktame padaliniių sąraše spaudžia pasirinkto padalinio juostoje esančią UPR-3 piktogramą. Sistema įvykdo komandą *remove* ir ištrina pasirinktą padalinį ir vertybių priežiūros grupės narys nukreipiamas į įstaigos struktūrinių duomenų sąrašą (2–6 žingsniai).

Įstaigų struktūriniuose padaliniuose esančių objektų sąrašas, esantis „Įstaigos“ meniu skyriaus „Objektais“ poskyryje, kaip ir meniu skyriaus „Įstaigos“ struktūrinių padaliniių sąrašas

valdomas naudojant ULMSR-1 maketo langą pagal sekų diagramos žingsnius (žr. 30 pav.), kuriuos vykdo vertybių priežiūros grupės narys naudodamas komandas: *office* – įstaigos struktūrinių padalinių objektų sąrašo peržiūrai (1–6 žingsniai), *addOffice* – naujo objekto įrašo sukūrimui spaudžiant „Sukurti“ mygtuką (7–26 žingsniai), *editOffice* – objekto duomenų keitimui (27–52 žingsniai), *removeOffice* – objekto įrašo ištrynimui (53–62 žingsniai).

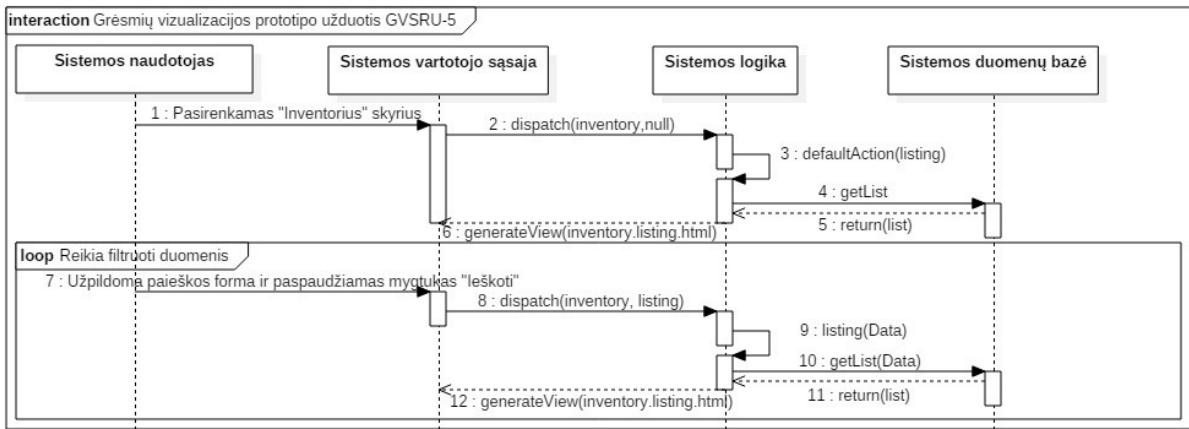
UFBR-4 Pagal GVSR-2 vartotojo sąsają užduoties GVSRU-4 vykdymo žingsniai atvaizduoti UML sekų diagramoje (žr. 30 pav.). Kaip ir UFBR-1 šioje sekų diagramoje pateikti ryšiai tarp tų pačių sistemos 4 elementų nenagrinėjant GVSR-1 vartotojo sąsajos dalies.

Vertybių grupės pavadinimų sąrašas, esantis „Vertybių“ meniu skyriaus „Grupės“ poskyryje, kaip ir meniu skyriaus „Įstaigos“ struktūrinių padalinių sąrašas valdomas naudojant ULMSR-1 maketo langą pagal sekų diagramos žingsnius (žr. 30 pav.), kuriuos vykdo vertybių priežiūros grupės narys naudodamas komandas: *group* – vertybių grupių sąrašo peržiūrai (1–6 žingsniai), *addGroup* – naujo vertybių grupės įrašo sukūrimui spaudžiant „Sukurti naują grupę“ mygtuką (7–26 žingsniai), *editGroup* – vertybių grupės duomenų keitimui (27–52 žingsniai), *removeGroup* – vertybių grupės įrašo ištrynimui (53–62 žingsniai).

Vertybių rūšies pavadinimų sąrašas, esantis „Vertybių“ meniu skyriaus „Rūšis“ poskyryje, kaip ir meniu skyriaus „Įstaigos“ struktūrinių padalinių sąrašas valdomas naudojant ULMSR-1 maketo langą pagal sekų diagramos žingsnius (žr. 30 pav.), kuriuos vykdo vertybių priežiūros grupės narys naudodamas komandas: *subgroup* – vertybių rūšies sąrašo peržiūrai (1–6 žingsniai), *addSubgroup* – naujo vertybių rūšies įrašo sukūrimui spaudžiant „Sukurti naują rūšį“ mygtuką (7–26 žingsniai), *editSubgroup* – vertybių rūšies duomenų keitimui (27–52 žingsniai), *removeSubgroup* – vertybių rūšies įrašo ištrynimui (53–62 žingsniai).

Vertybių pavadinimų sąrašas, esantis „Vertybių“ meniu skyriaus „Vertybių“ poskyryje, kaip ir meniu skyriaus „Įstaigos“ struktūrinių padalinių sąrašas valdomas naudojant ULMSR-1 maketo langą pagal sekų diagramos žingsnius (žr. 30 pav.), kuriuos vykdo vertybių priežiūros grupės narys naudodamas komandas: *listing* – vertybių sąrašo peržiūrai (1–6 žingsniai), *add* – naujo vertybių įrašo sukūrimui spaudžiant „Sukurti“ mygtuką (7–26 žingsniai), *edit* – vertybių duomenų keitimui (27–52 žingsniai), *remove* – vertybių įrašo ištrynimui (53–62 žingsniai).

UFBR-5 Pagal GVSR-2 vartotojo sasają užduoties GVSU-5 vykdymo žingsniai atvaizduoti UML sekų diagramose (žr. 30 ir 31 pav.). Kaip ir UFBR-1 šioje sekų diagramoje pateikti ryšiai tarp tų pačių sistemos 4 elementų nenagrinėjant GVSR-1 vartotojo sasajos dalies.



31 pav. GVSU-5 užduoties sekų diagramos dalis

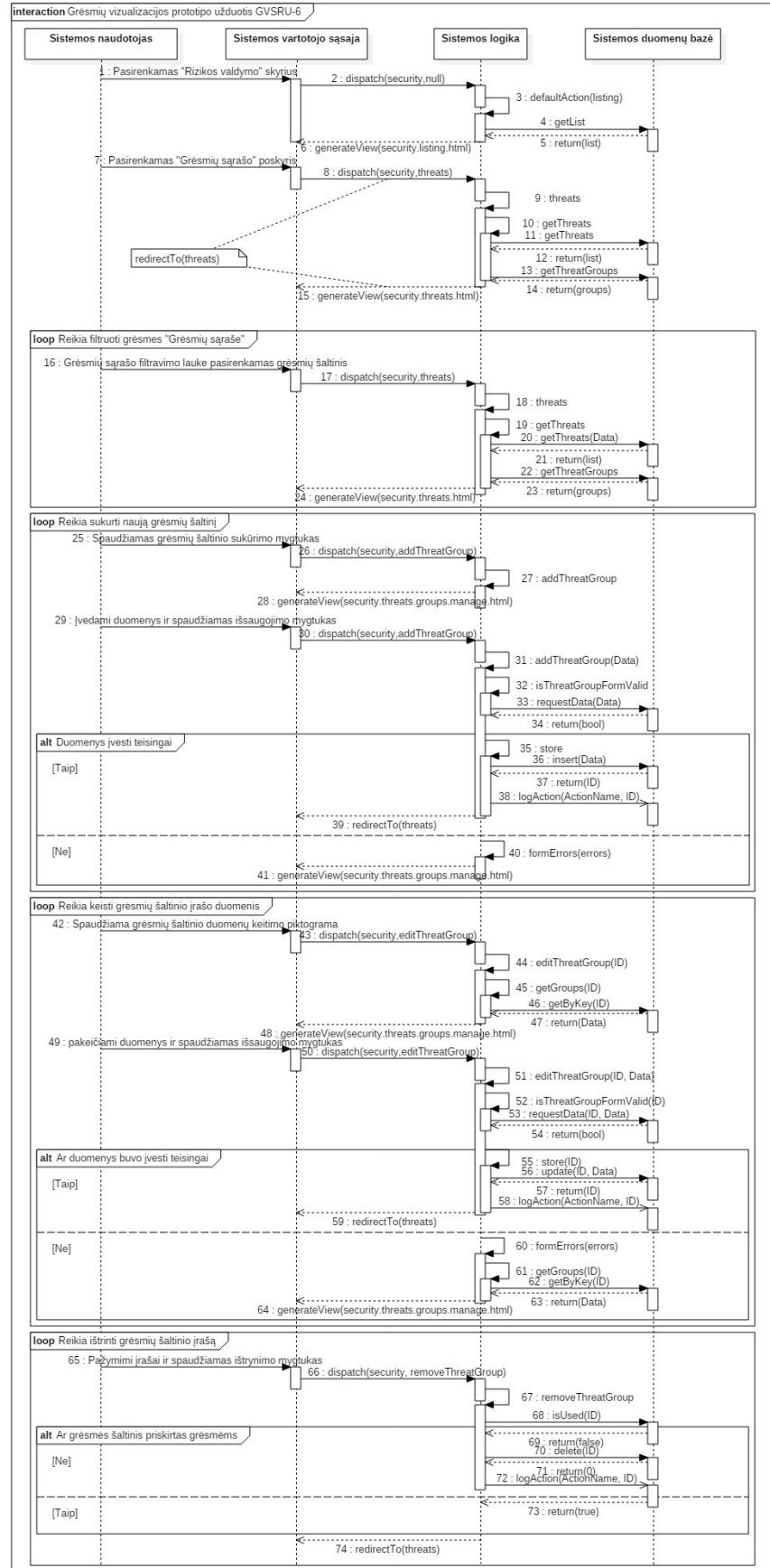
Dalis įstaigos inventoriaus sąrašo, esančio „Inventoriaus“ meniu skyriaus „Inventoriaus“ poskyryje, kaip ir „Įstaigos“ meniu skyriaus struktūrinių padalinių sąrašas valdomas naudojant ULMSR-3 maketo langą pagal sekų diagramos žingsnius (žr. 30 pav.), kuriuos vykdo vertybų priežiūros grupės narys naudodamas komandas: *listing* – įstaigos inventoriaus peržiūrai spaudžiant meniu skyrių „Inventorius“ (1–6 žingsniai), *add* – naujo inventoriaus įrašo sukūrimui spaudžiant „Sukurti įrašą“ mygtuką (7–26 žingsniai), *edit* – inventoriaus įrašo duomenų keitimui (27–52 žingsniai), *remove* – inventoriaus įrašo ištrynimui (53–62 žingsniai).

Įstaigos inventoriaus sąraše papildomai yra įdiegta galimybė atlikti duomenų paiešką, kurios žingsniai pateikti sekų diagramoje (žr. 31 pav.):

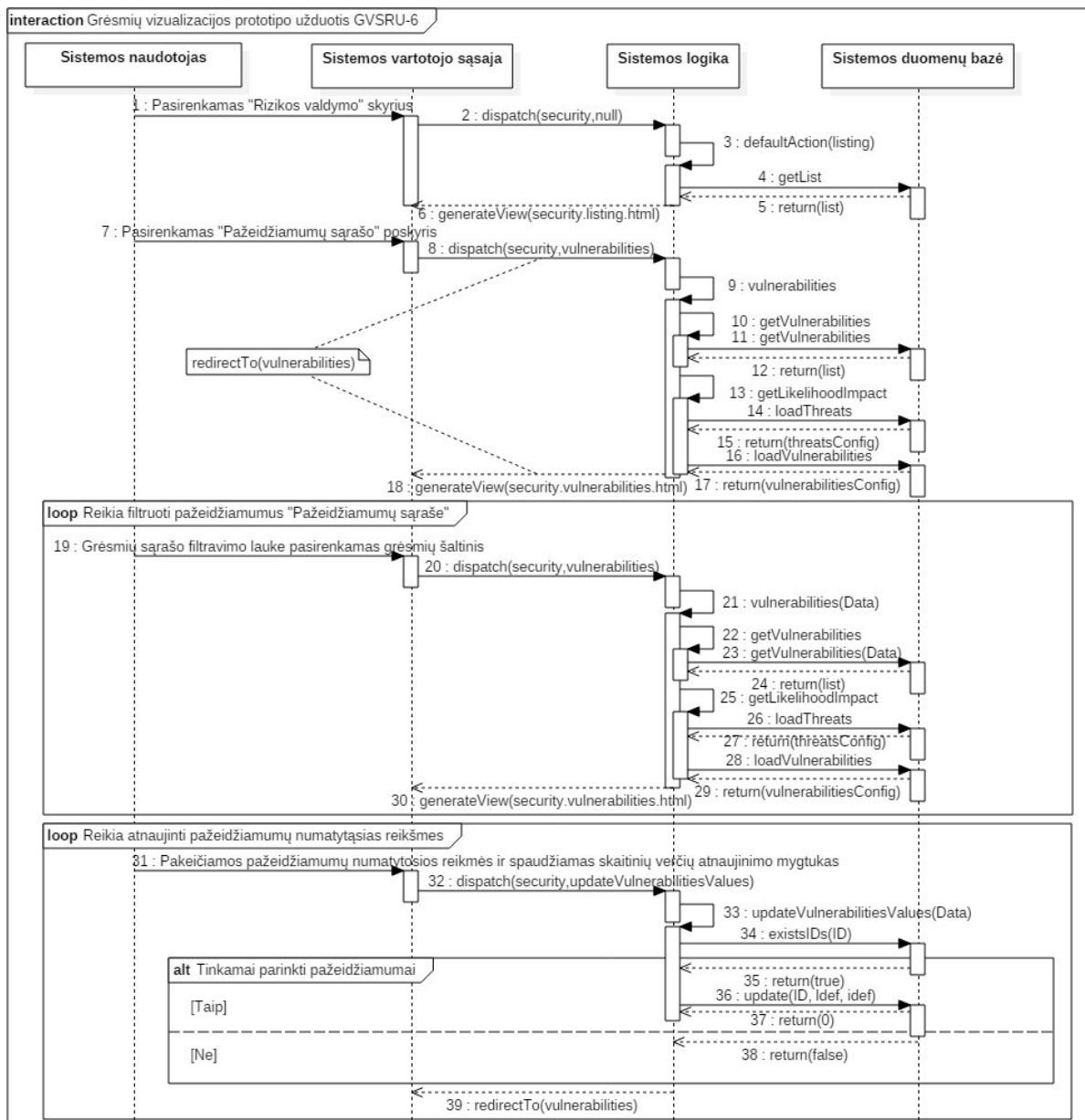
1–6 vertybų priežiūros grupės nariui pasirinkus meniu skyrių „Inventorius“ sistema pateikia įstaigų inventoriaus duomenis pagal GVSU-5 *listing* komanda suformuotą ULMSR-3 langą;

7–12 vertybų priežiūros grupės narys atlieka inventoriaus paiešką pasirinkdamas įstaigas ir (ar) užpildydamas paieškos formą ULMSR-3 lango paieškos organizavimo ir duomenų filtravimo vietoje, ir spausdamas „Paieškos“ mygtuką. Ši veiksmą vertybų priežiūros grupės narys kartojatol, kol gauna pageidaujamą paieškos rezultatą.

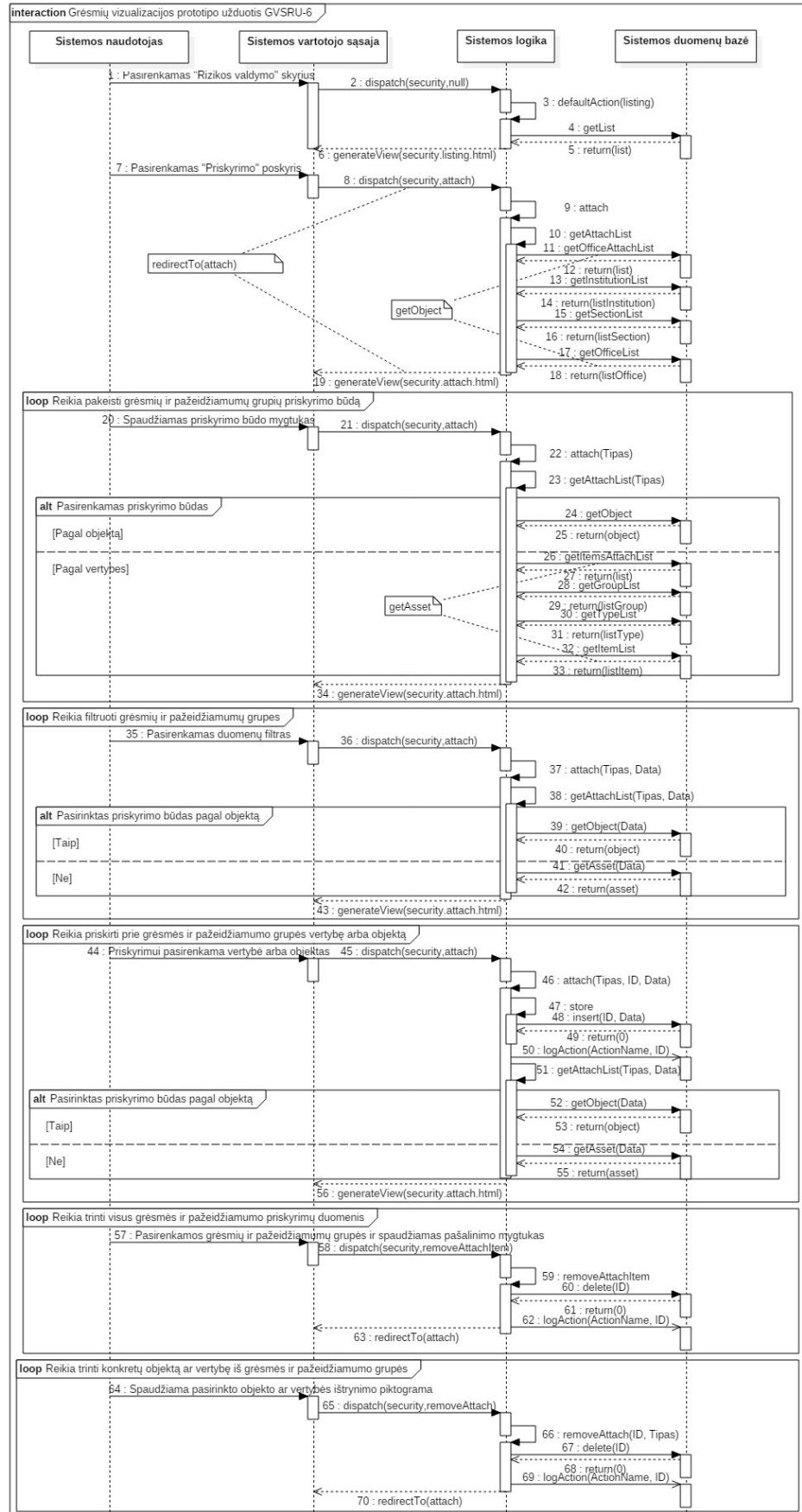
UFBR-6 Pagal GVSR-2 vartotojo sasają užduoties GVSU-6 vykdymo žingsniai atvaizduoti UML sekų diagramose (žr. 32, 33 ir 34 pav.). Kaip ir UFBR-1 šioje sekų diagramoje pateikti ryšiai tarp tų pačių sistemos 4 elementų nenagrinėjant GVSR-1 vartotojo sasajos dalies.



32 pav. GVSU-6 užduoties sekų diagramos dalis



33 pav. GVSU-6 užduoties sekų diagramos dalis



34 pav. GVSRU-6 užduoties sekų diagramos dalis

Sekų diagramoje (žr. 32 pav.) pateikiti sistemos elementų tarpusavio sąveikos žingsniai, kuriuos vykdo informacijos saugumo grupės narys siekdamas apibrėžti įstaigos vertybėms kylančias grėsmes, grėsmių šaltinius ir turimus pažeidžiamumus:

1–6 informacijos saugumo grupės nariui pasirinkus meniu skyrių „Rizikos valdymas“ sistema pateikia rizikos valdymo ataskaitų sąrašą pagal GVSRU-6 *listing* komanda suformuotą ULMSR-8 langą;

7–15 informacijos saugumo grupės nariui pasirinkus „Rizikos valdymo“ meniu skyriaus „Grėsmių sąrašo“ poskyrį sistema pateikia grėsmių šaltinių ir grėsmių sąrašo duomenis pagal GVSRU-6 *threats* komanda suformuotą ULMSR-4 langą;

16–24 informacijos saugumo grupės narys siekiantis filtruoti grėsmių sąrašo duomenis ULMSR-4 lango sąrašo filtravimo lauke pasirenka grėsmių šaltinį ir sistema įvykdo *threats* komandą, kuri į ekraną išveda grėsmių sąrašo duomenis pagal pasirinktą grėsmės šaltinį;

25–28 informacijos saugumo grupės narys siekiantis sukurti naują grėsmės šaltinio įrašą spaudžia mygtuką „Sukurti naują grėsmių šaltinį“ ir inicijuoja *addThreatGroup* komandos vykdymą, sistema pateikia ULMDR-1 duomenų įvesties langą;

29–34 informacijos saugumo grupės narys įvedęs formos duomenis spaudžia ULMDR-1 veiksmų juostoje esantį duomenų išsaugojimo mygtuką, tada sistemoje pakartotinai inicijuojamas *addThreatGroup* komandos vykdymas, tikrinami įvesti duomenys (įvesti atitinkami formos laukai yra netušti, unikalūs ir nepasikartojantys);

35–39 jeigu duomenys yra įvesti taisyklingai, tada sistema išsaugoja grėsmės šaltinio duomenų įrašą kartu su atlikto veiksmo žyme duomenų bazėje ir nukreipia informacijos saugumo grupės narį į grėsmių sąrašą (7–15 žingsniai);

40–41 jeigu įvedami duomenys netaisyklingai ULMDR-1 klaidos pranešimo vietoje atvaizduoja pranešimą apie įvykusią klaidą ir kartojančias žingsnis nuo 29;

42–48 informacijos saugumo grupės narys siekiantis keisti grėsmės šaltinio duomenis ULMSR-4 lange pasirinkto šaltinio juostoje spaudžia UPR-2 piktogramą, kuri įvykdo *editThreatGroup* komandą ir pateikia ULMDR-1 duomenų įvesties langą;

49–54 informacijos saugumo grupės narys pakeičia grėsmės šaltinio duomenis ir spaudžia ULMDR-1 veiksmų juostoje esantį duomenų išsaugojimo mygtuką. Vykdoma *editThreatGroup* komanda bei apdorojami formoje įvesti ar pakeisti duomenys;

55–59 jeigu įvesti duomenys atitinka sistemos reikalavimus (įvesti atitinkami formos laukai yra netušti, unikalūs ir nepasikartojantys), tada vykdomas grėsmės šaltinio duomenų

atnaujinimas. Lygiagrečiai išsaugojamas žurnalinis įrašas apie informacijos saugumo grupės nario atliktą veiksmą ir vykdomas vartotojo sąsajos nukreipimas į grėsmių šaltinių ir grėsmių sąrašą (7–15 žingsniai);

60–64 jeigu duomenys yra įvesti netaisyklingai ULMDR-1 klaidos pranešimo vietoje sistema atvaizduoja pranešimą apie įvykusią klaidą ir kartojamas žingsnis nuo 49;

65–74 informacijos saugumo grupės narys siekiantis ištinti neberekalingą grėsmės šaltinį ULMSR-4 lange pateiktame grėsmės šaltinių sąraše spaudžia pasirinkto šaltinio juostoje esančią UPR-3 piktogramą. Sistema įvykdo komandą *removeThreatGroup* ir iština pasirinktą šaltinį ir informacijos saugumo grupės narys nukreipiamas į grėsmės šaltinių ir grėsmių sąrašą (7–15 žingsniai). Ištinti grėsmės šaltinį leidžiama, jeigu prie jo nėra priskirtų grėsmių.

Grėsmių sąrašas, esantis „Rizikos valdymo“ meniu skyriaus „Grėsmių sąrašo“ poskyryje, kaip ir to pačio poskyrio grėsmių šaltinių sąrašas valdomas naudojant ULMSR-4 maketo langą pagal sekų diagramos žingsnius (žr. 32 pav.), kuriuos vykdo informacijos saugumo grupės narys naudodamas komandas: *addThreat* – naujos grėsmės įrašo sukūrimui spaudžiant „Sukurti naują grėsmę“ mygtuką ir papildomai tikrinant įvestų grėsmės šaltinių identifikacinius numerius (25–41 žingsniai), *addVulnerabilities* – naujo pažeidžiamumo įrašo sukūrimui spaudžiant „Sukurti pažeidžiamumą pasirinktai grėsmei“ mygtuką ir papildomai tikrinant įvestų grėsmių identifikacinius numerius (25–41 žingsniai), *editThreat* – grėsmės įrašo duomenų keitimui papildomai tikrinant įvestų grėsmės šaltinių identifikacinius numerius (42–64 žingsniai), *removeThreat* – grėsmės įrašo ištrynimui kur trinti leidžiama tik prie grėsmės nėra priskirtų pažeidžiamumų (65–74 žingsniai).

Dalis pažeidžiamumų sąrašo, esančio „Rizikos valdymo“ meniu skyriaus „Pažeidžiamumų sąrašo“ poskyryje, kaip ir grėsmių šaltinių sąrašas valdomas naudojant ULMSR-5 maketo langą pagal sekų diagramos žingsnius (žr. 32 pav.), kuriuos vykdo informacijos saugumo grupės narys naudodamas komandas: *editVulnerabilities* – pažeidžiamumo įrašo duomenų keitimui papildomai tikrinant įvestų grėsmių identifikacinius numerius (42–64 žingsniai), *removeVulnerabilities* – pažeidžiamumo įrašo ištrynimui (65–74 žingsniai).

Sekų diagramoje (žr. 33 pav.) pateiki sistemos elementų tarpusavio sąveikos žingsniai, kuriuos vykdo informacijos saugumo grupės narys siekdamas valdyti galimų pažeidžiamumų duomenis:

1–6 informacijos saugumo grupės nariui pasirinkus meniu skyrių „Rizikos valdymas“ sistema pateikia rizikos valdymo ataskaitų sąrašą pagal GVSRU-6 *listing* komanda suformuotą ULMSR-8 langą;

7–18 informacijos saugumo grupės nariui pasirinkus „Rizikos valdymo“ meniu skyriaus „Pažeidžiamumų sąrašo“ poskyrių sistema pateikia grėsmių ir pažeidžiamumų grupių duomenis pagal GVSRU-6 *vulnerabilities* komanda suformuotą ULMSR-5 langą;

19–30 informacijos saugumo grupės narys atlieka pažeidžiamumų sąrašo filtravimą pasirinkdamas reikšmes iš grėsmių ir grėsmės šaltinių galimų reikšmių, kurios atvaizduojamos ULMSR-5 lango sąrašo filtravimo vietoje. Ši veiksmą vertybų priežiūros grupės narys kartoja tol, kol gauna pageidaujamą grėsmių ir pažeidžiamumų grupių sąrašo rezultatą;

31–34 informacijos saugumo grupės narys siekdamas atnaujinti grėsmių ir pažeidžiamumų grupių pasireiškimo tikimybes bei galimą poveikį pakeičia numatytuosius parametrus grėsmių ir pažeidžiamumų grupių sąraše ir spaudžia ULMSR-5 lango veiksmų mygtuką „Atnaujinti skaitines vertes“. Sistema atlieka tikrinimą, ar tinkamai yra pasirinkti pažeidžiamumų identifikacioniniai numeriai;

35–37 jeigu tinkamai pasirinkti identifikacioniniai numeriai, tada atnaujina pakeistąsias tikimybės ir poveikio reikšmes;

38–39 sistema vykdo vartotojo sąsajos nukreipimą į grėsmių ir pažeidžiamumų grupių sąrašą (8–18 žingsniai).

Sekę diagramoje (žr. 34 pav.) pateiki sistemos elementų tarpusavio sąveikos žingsniai, kuriuos vykdo informacijos saugumo grupės narys siekdamas priskirti grėsmių ir pažeidžiamumų grupes prie turimų vertybų ar pasireiškimo vietos:

1–6 informacijos saugumo grupės nariui pasirinkus meniu skyrių „Rizikos valdymas“ sistema pateikia rizikos valdymo ataskaitų sąrašą pagal GVSRU-6 *listing* komanda suformuotą ULMSR-8 langą;

7–19 informacijos saugumo grupės nariui pasirinkus „Rizikos valdymo“ meniu skyriaus „Priskyrimo“ poskyrių sistema šiam sistemos naudotojui pateikia grėsmių ir pažeidžiamumų grupių priskyrimo prie atitinkamų įstaigų, struktūrinių padalinių ar jų objektų sąrašo duomenis pagal GVSRU-6 *attach* komanda suformuotą ULMSR-6 langą;

20–23 informacijos saugumo grupės narys siekdamas pasirinkti grėsmių ir pažeidžiamumų grupių priskyrimą prie disponuojamų vertybų, jų grupių ir rūšių, spaudžia ULMSR-6 lango priskyrimo būdo pasirinkimo vietoje mygtuką „Priskirti vertynes“, o prie atitinkamų įstaigų, struktūrinių padalinių ar jų objektų – „Priskirti vietą“;

24–33 atitinkamai nuo informacijos saugumo grupės nario priskyrimo būdo pasirinkimo sistema inicijuoja atitinkamas komandas į duomenų bazę ir gautus duomenis grąžina sistemos vartotojo sasajai;

34 informacijos saugumo grupės nariui sistema ULMSR-6 lange suformuoja grėsmių ir pažeidžiamumų grupių priskyrimo duomenis;

35–38 informacijos saugumo grupės narys siekdamas filtruoti grėsmių ir pažeidžiamumų grupių priskyrimo duomenis sąrašo filtravimo lauke pasirenka atitinkamą grėsmės šaltinio ir (ar) grėsmės reikšmę;

39–42 atitinkamai nuo informacijos saugumo grupės nario priskyrimo būdo pasirinkimo sistema inicijuoja atitinkamas komandas į duomenų bazę ir gautus duomenis grąžina sistemos vartotojo sasajai;

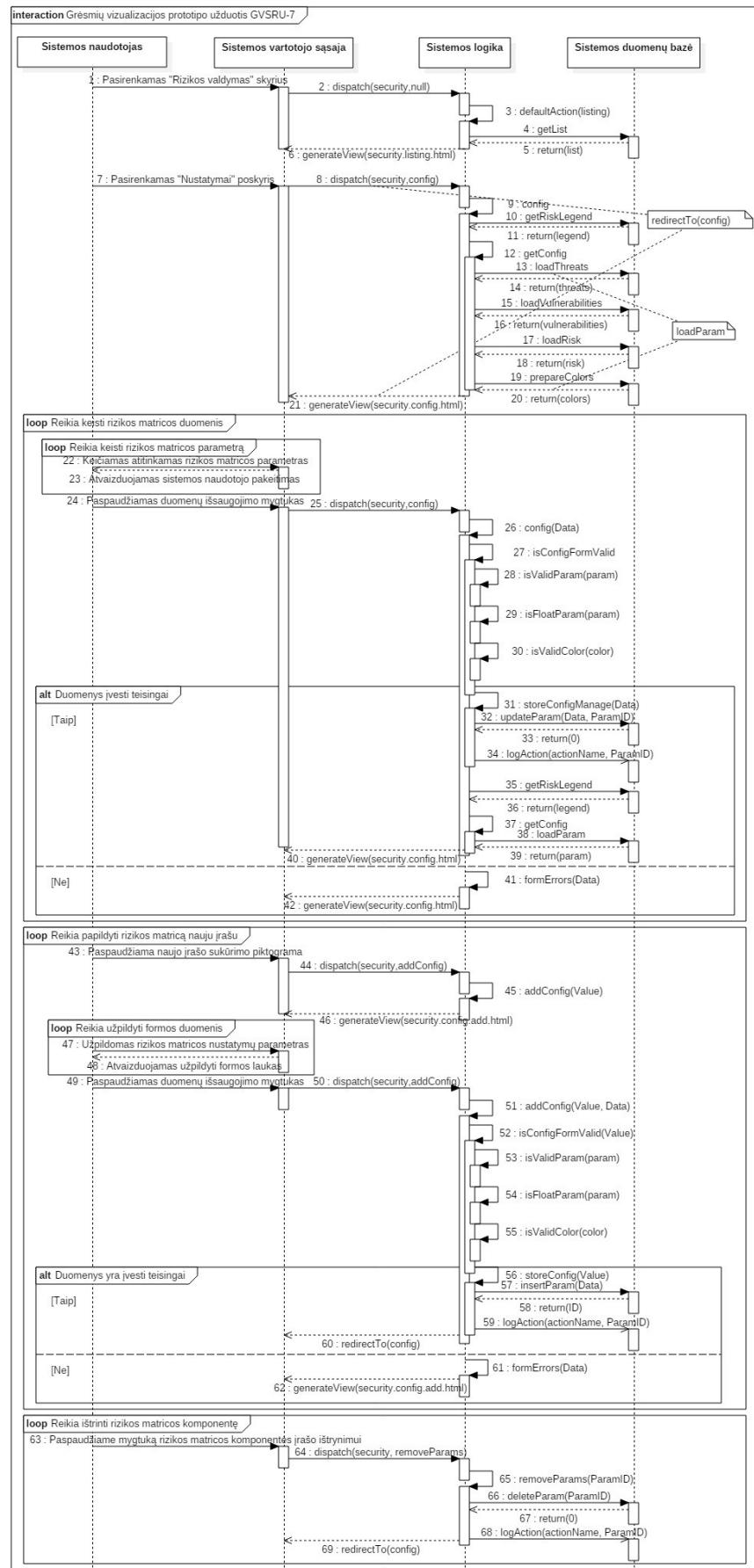
43 informacijos saugumo grupės nariui sistema ULMSR-6 lange suformuoja filtruotus grėsmių ir pažeidžiamumų grupių priskyrimo duomenis;

44–56 informacijos saugumo grupės narys siekdamas priskirti tam tikrą vertybės ar vienos parametru prie grėsmės ir pažeidžiamumo grupės ši priskyrimą atlieka ULMSR-6 lango priskyrimo sąrašu vietoje, kurį sistema kartu su atlikto veiksmo žyme išsaugoja priklausomai nuo pasirinkto priskyrimo būdo;

57–63 informacijos saugumo grupės narys siekdamas pašalinti visus vertybės ar vienos parametrus nuo grėsmės ir pažeidžiamumo grupės pažymi atitinkamas grupes ir ULMSR-6 lange spaudžia veiksmų mygtuką „Pašalinti“. Sistema nuo grėsmės ir pažeidžiamumo grupių pašalina visus vertybės (komanda *removeAttachItem*) ar vienos (komanda *removeAttachPlace*) parametrus ir išsaugoja atlikto veiksmo žymę, nukreipia vartotojo sasają į grėsmių ir pažeidžiamumų grupių priskyrimo sąrašą (8–19 žingsniai);

64–70 informacijos saugumo grupės narys siekdamas pašalinti grėsmės ir pažeidžiamumo grupei priskirtą konkretų vertybės ar vienos parametru ULMSR-6 lango priskyrimo sąrašu vietoje spaudžia atitinkamą UPR-3 piktogramą. Sistema vykdyma komandą *removeAttach* pašalina ši parametru ir išsaugoja atlikto veiksmo žymę, nukreipia vartotojo sasają į grėsmių ir pažeidžiamumų grupių priskyrimo sąrašą (8–19 žingsniai).

UFBR-7 Pagal GVSR-2 vartotojo sasają užduoties GVSRU-7 vykdymo žingsniai atvaizduoti UML sekų diagramoje (žr. 35 pav.). Kaip ir UFBR-1 šioje sekų diagramoje pateikti ryšiai tarp tų pačių sistemos 4 elementų nenagrinėjant GVSR-1 vartotojo sasajos dalies.



35 pav. GVSRU-7 užduoties sekų diagrama

Sekų diagramoje (žr. 35 pav.) pateikiti sistemos elementų tarpusavio sąveikos žingsniai, kuriuos vykdo informacijos saugumo grupės narys siekdamas nustatyti apsibrėžtus grėsmės ir pažeidžiamumo grupių pasireiškimo tikimybės, poveikio ir rizikos parametrus:

1–6 informacijos saugumo grupės nariui pasirinkus meniu skyrių „Rizikos valdymas“ sistema pateikia rizikos valdymo ataskaitų sąrašą pagal GVSRU-7 *listing* komanda suformuotą ULMSR-8 langą;

7–21 informacijos saugumo grupės nariui pasirinkus „Rizikos valdymo“ meniu skyriaus „Nustatymai“ poskyrį sistema šiam sistemos naudotojui *config* komanda pateikia visus grėsmės ir pažeidžiamumo grupių pasireiškimo tikimybės, poveikio ir rizikos parametrus pagal GVSRU-7 *config* komanda suformuotą ULMSR-7 langą;

22–30 informacijos saugumo grupės narys siekdamas pakeisti esamus grėsmės ir pažeidžiamumo grupių pasireiškimo tikimybės, poveikio ir rizikos parametrus juos formos laukuose pakeičia ir GVSRU-7 lange spaudžia veiksmų mygtuką „Išsaugoti“. Sistema vykdo komandą *config* ir atlieka įvestų duomenų patikrinimą;

31–40 jeigu duomenys yra įvesti taisyklingai (tinkamos formos, slankaus kablelio ir spalvos reikšmės), tada jie išsaugojami sistemos duomenų bazėje kartu su atlikto veiksmo žyma ir atvaizduoja sėkmingo duomenų atnaujinimo pranešimą ULMSR-7 lango sistemos pranešimo vietoje;

41–42 jeigu duomenys yra įvesti netaisyklingai sistema formuoja klaidos pranešimą ULMSR-7 lango sistemos pranešimo vietoje. Informacijos saugumo grupės narys kartoja žingsnį nuo 22;

43–46 informacijos saugumo grupės narys siekdamas papildyti naujas grėsmės ir pažeidžiamumo grupių pasireiškimo tikimybės, poveikio ir rizikos parametrais spaudžia atitinkamą ULMSR-7 lango UPR-7 piktogramą. Sistema atitinkamai vykdo komandą *addConfig* ir pateikia informacijos saugumo grupės nariui ULMDR-1 duomenų įvesties langą;

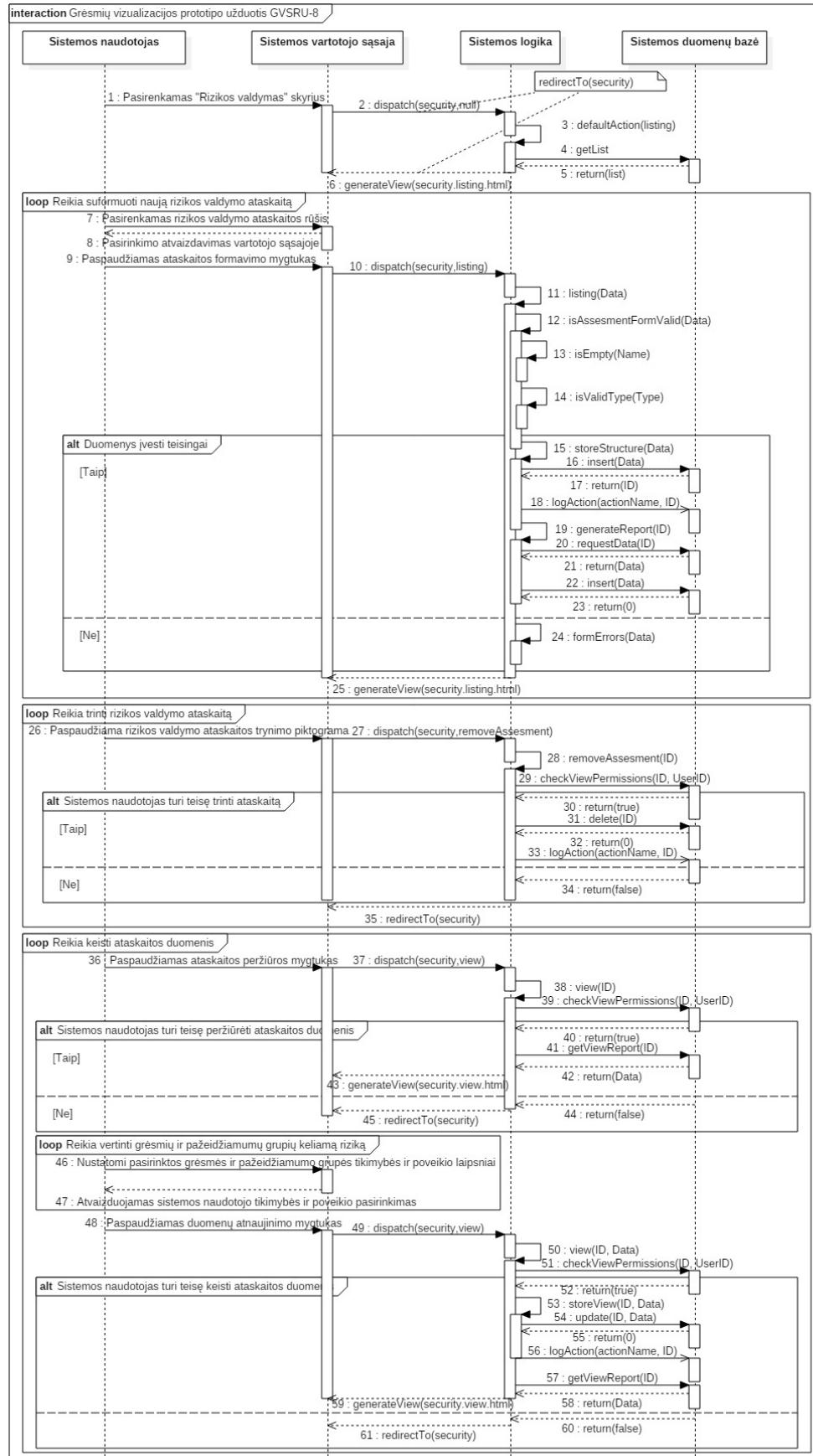
47–55 informacijos saugumo grupės narys užpildo gautą ULMDR-1 duomenų įvesties langą ir spaudžia veiksmų mygtuką „Išsaugoti“. Sistema vykdo komandą *addConfig* ir atlieka įvestų duomenų patikrinimą;

56–60 jeigu duomenys yra įvesti taisyklingai (tinkamos formos, slankaus kablelio ir spalvos reikšmės), tada jie išsaugojami sistemos duomenų bazėje kartu su atlikto veiksmo žyma ir vartotojo sėsaja nukreipiama į grėsmės ir pažeidžiamumo grupių pasireiškimo tikimybės, poveikio ir rizikos parametru sąrašą (8–21 žingsniai);

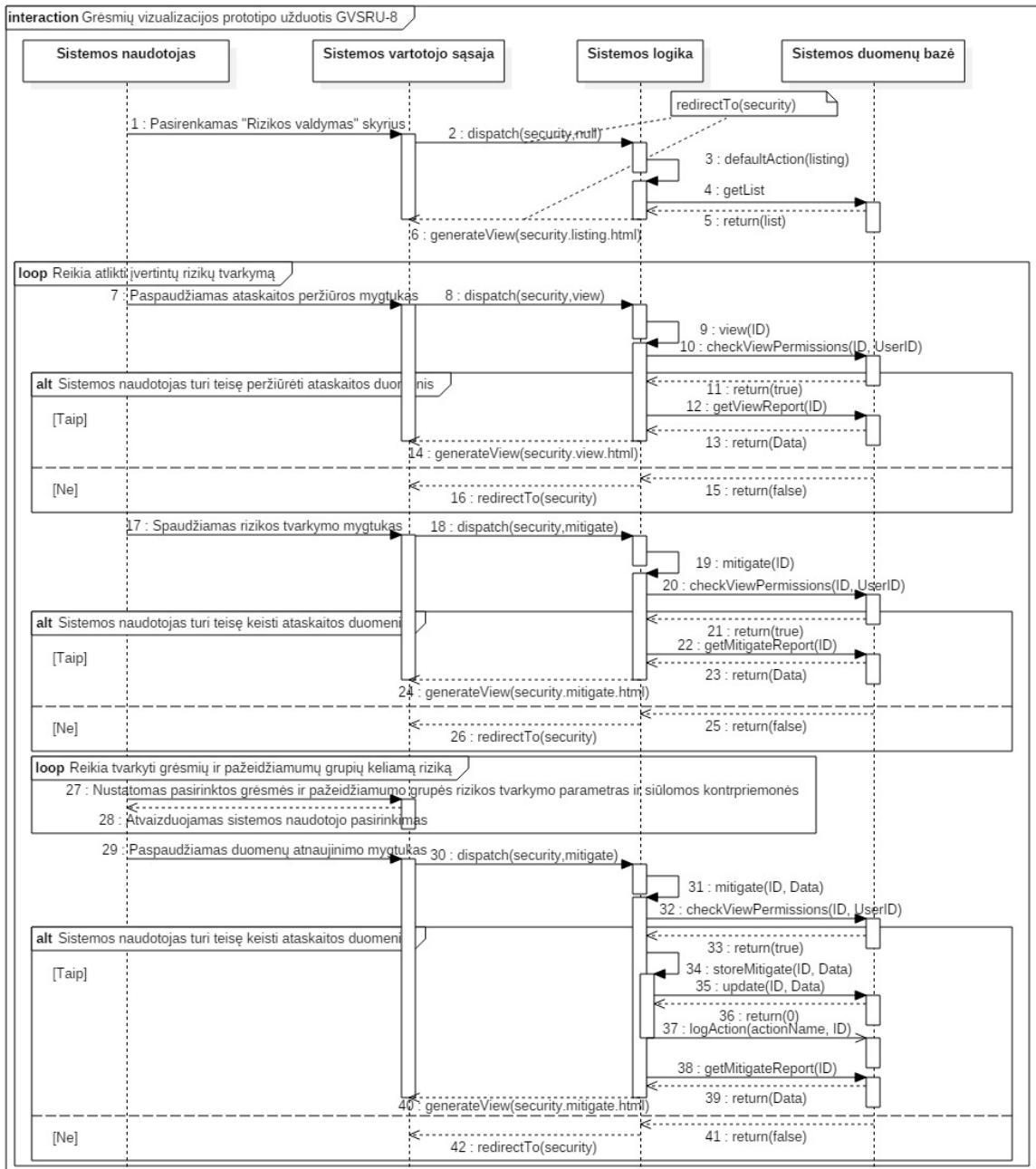
61–62 jeigu duomenys yra įvesti netaisyklingai sistema formuoja klaidos pranešimą ULMDR-1 duomenų įvesties lango klaidos pranešimo vietoje. Informacijos saugumo grupės narys kartoja žingsnį nuo 47;

63–69 informacijos saugumo grupės narys siekdamas pašalinti grėsmės ir pažeidžiamumo grupių pasireiškimo tikimybės, poveikio ar rizikos parametru ULMSR-7 lango piktogramų vietoje spaudžia atitinkamą UPR-3 piktogramą. Sistema vykdyma *removeLikelihoodConfig*, *removeImpactConfig*, *removeRiskConfig* komandas atitinkamai pašalina pasirinktą tikimybės, poveikio ar rizikos parametru, išsaugoja atlikto veiksmo žymę bei nukreipia vartotojo sasają į grėsmės ir pažeidžiamumo grupių pasireiškimo tikimybės, poveikio ir rizikos parametrų sąrašą (8–21 žingsniai).

UFBR-8 Pagal GVSR-2 vartotojo sasają užduoties GVSRU-8 vykdymo žingsniai atvaizduoti UML sekų diagramose (žr. 36 ir 37 pav.). Kaip ir UFBR-1 šioje sekų diagramoje pateikti ryšiai tarp tų pačių sistemos 4 elementų nenagrinėjant GVSR-1 vartotojo sasajos dalies.



36 pav. GVSRU-8 užduoties sekų diagramos dalis



37 pav. GVSU-8 užduoties sekų diagramos dalis

Sekų diagramoje (žr. 36 pav.) pateikiti sistemos elementų tarpusavio sąveikos žingsniai, kuriuos vykdo informacijos saugumo grupės narys siekdamas formuoti ištaigos rizikos valdymo ataskaitą ir įvertinti grėsmių ir pažeidžiamumų grupes:

1–6 informacijos saugumo grupės nariui pasirinkus meniu skyrių „Rizikos valdymas“ sistema pateikia rizikos valdymo ataskaitų sąrašą pagal GVSU-8 *listing* komanda suformuotą ULMSR-8 langą;

7–14 informacijos saugumo grupės narys siekdamas suformuoti rizikos valdymo ataskaitą pasirenka ataskaitos rūšį, įrašo ataskaitos pavadinimą ir ULMSR-8 lange spaudžia rizikos

valdymo formos mygtuką „Pradėti“. Sistema vykdo komandą *listing* ir atlieka įvestų duomenų patikrinimą;

15–23 jeigu formos duomenys yra įvesti taisyklingai (tinkama ataskaitos rūšis ir užpildytas ataskaitos laukas), tada pagal dabartinę inventoriaus situaciją sistema suformuoja ataskaitos duomenis, kuriuos išsaugoja duomenų bazėje, taip pat išsaugant atlikto veiksmo žymą;

24 jeigu duomenys yra įvesti netaisyklingai sistema ruošia klaidos pranešimą ULMSR-8 klaidos pranešimo vietoje;

25 vartotojo sasajoje atvaizduojamas rizikos valdymo ataskaitų sąrašas;

26–29 informacijos saugumo grupės narys siekdamas ištrinti vieną ataskaitą iš rizikos valdymo ataskaitų sąrašo ULMSR-8 lange spaudžia šios ataskaitos juostoje esančią UPR-3 piktogramą. Sistema vykdo komandą *removeAssesment* ir atlieka rizikos valdymo ataskaitos teisių patikrinimą;

30–33 jeigu informacijos saugumo grupės nariui priklauso trinama ataskaita, tada pasirinktos ataskaitos duomenys yra ištrinami iš duomenų bazės, išsaugojama atlikta veiksmo žyma;

34 jeigu informacijos saugumo grupės nariui nepriklauso trinama ataskaita, tada ataskaitos duomenys yra netrinami;

35 vartotojo sasaja nukreipiama į rizikos valdymo ataskaitų sąrašą (2–6 žingsniai);

36–39 informacijos saugumo grupės narys siekdamas peržiūrėti ir pakeisti suformuotos rizikos valdymo ataskaitos duomenis ULMSR-8 lange spaudžia ataskaitos peržiūros mygtuką. Sistema vykdo komandą *view* ir atlieka rizikos valdymo ataskaitos teisių patikrinimą;

40–43 jeigu informacijos saugumo grupės nariui priklauso peržiūrima ataskaita, tada vykdoma komanda *getViewReport* ir informacijos saugumo grupės narys nukreipiama į grėsmių ir pažeidžiamumų grupių rizikos vertinimo langą ULMSR-9;

44–45 jeigu informacijos saugumo grupės nariui nepriklauso peržiūrima ataskaita, tada vartotojo sasaja nukreipiama į rizikos valdymo ataskaitų sąrašą (2–6 žingsniai);

46–51 informacijos saugumo grupės narys siekdamas keisti suformuotas rizikos valdymo ataskaitos duomenis ir atlikti rizikos vertinimą ULMSR-9 lange nustato grėsmių ir pažeidžiamumų grupių pasireiškimo tikimybes ir poveikio parametrus ir spaudžia veiksmų mygtuką „Atnaujinti“. Sistema vykdo komandą *view* ir atlieka rizikos valdymo ataskaitos teisių patikrinimą;

52–59 jeigu informacijos saugumo grupės nariui priklauso keičiamą ataskaitą, tada išsaugojami atnaujinti grėsmių ir pažeidžiamumų pasireiškimo tikimybių ir poveikio parametrai ir atvaizduojami ULMSR-9 lange atnaujinti grėsmių ir pažeidžiamumų grupių rizikos vertinimo duomenys;

60–61 jeigu informacijos saugumo grupės nariui nepriklauso peržiūrima ataskaita, tada vartotojo sasaja nukreipiama į rizikos valdymo ataskaitų sąrašą (2–6 žingsniai);

Sekę diagramoje (žr. 37 pav.) pateiki sistemos elementų tarpusavio sąveikos žingsniai, kuriuos vykdo informacijos saugumo grupės narys siekdamas tvarkytį nepriimtiną riziką ir atliskti rizikos mažinimo procedūrą:

1–6 informacijos saugumo grupės nariui pasirinkus meniu skyrių „Rizikos valdymas“ sistema pateikia rizikos valdymo ataskaitų sąrašą pagal GVSRU-8 *listing* komanda suformuotą ULMSR-8 langą;

7–10 informacijos saugumo grupės narys siekdamas peržiūrėti ir įvykdyti grėsmių ir pažeidžiamumų grupių keliamos rizikos tvarkymą ULMSR-8 lange spaudžia pasirinktos rizikos valdymo ataskaitos peržiūros mygtuką. Sistema vykdo komandą *view* ir atlieka rizikos valdymo ataskaitos teisių patikrinimą;

11–14 jeigu informacijos saugumo grupės nariui priklauso peržiūrima ataskaita, tada vykdoma komanda *getViewReport* ir informacijos saugumo grupės narys nukreipiama į langą ULMSR-9;

15–16 jeigu informacijos saugumo grupės nariui nepriklauso peržiūrima ataskaita, tada vartotojo sasaja nukreipiama į rizikos valdymo ataskaitų sąrašą (2–6 žingsniai);

17–20 informacijos saugumo grupės narys siekdamas peržiūrėti ir tvarkytį grėsmių ir pažeidžiamumų grupių keliamą riziką ULMSR-9 lange spaudžia rizikos valdymo dalies mygtuką „Rizikos tvarkymas“. Sistema vykdo komandą *mitigate* ir atlieka rizikos valdymo ataskaitos teisių patikrinimą;

21–24 jeigu informacijos saugumo grupės nariui priklauso peržiūrima ataskaita, tada vykdoma komanda *getMitigateReport* ir informacijos saugumo grupės narys nukreipiama į grėsmių ir pažeidžiamumų grupių keliamos rizikos tvarkymo langą ULMSR-9;

25–26 jeigu informacijos saugumo grupės nariui nepriklauso peržiūrima ataskaita, tada vartotojo sasaja nukreipiama į rizikos valdymo ataskaitų sąrašą (2–6 žingsniai);

27–32 informacijos saugumo grupės narys siekdamas tvarkyti grėsmių ir pažeidžiamumų grupių keliamą riziką ULMSR-9 lange visoms grėsmių ir pažeidžiamumų grupėms nuo didžiausios rizikos iki mažiausios atlieka rizikos tvarkymo procedūrą. Informacijos saugumo grupės narys pasirenka rizikos tvarkymo būdą ir reikalingas įdiegti kontrpriemones rizikos mažinimui, ir spaudžia veiksmų mygtuką „Atnaujinti“. Sistema vykdo komandą *mitigate* ir atlieka rizikos valdymo ataskaitos teisių patikrinimą;

33–40 jeigu informacijos saugumo grupės nariui priklauso peržiūrima ataskaita, tada atnaujinami rizikos tvarkymo duomenys, išsaugojama atlanko veiksmo žymė ir atvaizduojami ULMSR-9 lange atnaujinti grėsmių ir pažeidžiamumų grupių keliamos rizikos tvarkymo duomenys;

41–42 jeigu informacijos saugumo grupės nariui nepriklauso peržiūrima ataskaita, tada vartotojo sėsaja nukreipiama į rizikos valdymo ataskaitų sąrašą (2–6 žingsniai).