VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
FUNDAMENTINIŲ MOKSLŲ FAKULTETAS
INFORMACINIŲ SISTEMŲ KATEDRA

Rytis Šakalys

MCDM METODŲ TAIKYMAS REGISTRŲ IR INFORMACINIŲ SISTEMŲ SPECIFIKACIJŲ SAUGUMO REIKALAVIMŲ KOKYBEI VERTINTI

APPLICATION OF MCDM METHODS TO EVALUATE THE QUALITY OF SECURITY REQUIREMENTS FOR REGISTRIES AND INFORMATION SYSTEM SPECIFICATIONS

Baigiamasis magistro darbas

Informacijos ir informacinių technologijų saugos studijų programa, valstybinis kodas
6211BX008
Informatikos inžinerijos studijų kryptis

Vilnius, 2025

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
FUNDAMENTINIŲ MOKSLŲ FAKULTETAS
INFORMACINIŲ SISTEMŲ KATEDRA

Rytis Šakalys

MCDM METODŲ TAIKYMAS REGISTRŲ IR INFORMACINIŲ SISTEMŲ SPECIFIKACIJŲ SAUGUMO REIKALAVIMŲ KOKYBEI VERTINTI

APPLICATION OF MCDM METHODS TO EVALUATE THE QUALITY OF SECURITY REQUIREMENTS FOR REGISTRIES AND INFORMATION SYSTEM SPECIFICATIONS

Baigiamasis magistro darbas

Informacijos ir informacinių technologijų saugos studijų programa, valstybinis kodas
6211BX008
Informatikos inžinerijos studijų kryptis

Vadovas	dr. Donatas Vitkus (Moksl. laipsnis/pedag. vardas, vardas, pavardė)
Lietuvių kalbos konsultantas	dr. Vaida Buivydienė (Moksl. laipsnis/pedag. vardas, vardas, pavardė)

Vilnius, 2025

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Rytis Šakalys, 20231547

(Studento vardas ir pavardė, studento pažymėjimo Nr.)

Fundamentinių mokslų fakultetas

(Fakultetas)

Informacijos ir informacinių technologijų sauga, ITSfm-23

(Studijų programa, akademinė grupė)

BAIGIAMOJO DARBO (PROJEKTO) SĄŽININGUMO DEKLARACIJA

2025 m. gegužės 28 d.

Patvirtinu, kad mano baigiamasis darbas tema „MCDM metodų taikymas registrų ir informacinių sistemų specifikacijų saugumo reikalavimų kokybei vertinti“ yra savarankiškai parašytas. Šiame darbe pateikta medžiaga nėra plagijuota. Tiesiogiai ar netiesiogiai panaudotos kitų šaltinių citatos pažymėtos literatūros nuorodose.

Parenkant ir įvertinant medžiagą bei rengiant baigiamąjį darbą, mane konsultavo mokslininkai ir specialistai: daktaras Vaida Buivydienė. Mano darbo vadovas daktaras Donatas Vitkus.

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

Rytis Šakalys

(Parašas) (Vardas ir pavardė)

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
FUNDAMENTINIŲ MOKSLŲ FAKULTETAS
INFORMACINIŲ SISTEMŲ KATEDRA

Studijų kryptis: Informatikos inžinerija
Studijų programa: Informacijos ir informacinių technologijų sauga , valstybinis kodas 6211BX014
Specializacija: Informacijos ir informacinių technologijų sauga

TVIRTINU
Katedros vedėjas
Nikolaj Goranin
2025-05-29

MAGISTRO BAIGIAMOJO DARBO UŽDUOTIS

Nr. ITSfm-23–11303

Vilnius

Studentas (-ė): Rytis Šakalys

Baigiamojo darbo tema: MCDM metodų taikymas registrų ir informacinių sistemų specifikacijų saugumo reikalavimų kokybei vertinti

Baigiamojo darbo užbaigimo terminas pagal numatytą studijų kalendorinį grafiką.

BAIGIAMOJO DARBO UŽDUOTIS:

Tikslas: Darbo tikslas – patobulinti registro ir informacinės sistemos saugumo reikalavimų kokybės vertinimą, taikant daugiakriterius sprendimo priėmimo metodus.

Uždaviniai:
1. Atlikti registrų ir informacinių sistemų saugumo reikalavimų ir jų kokybės gerinimo analizę, kartu pristatant daugiakriterius metodus;
2. Pasiūlyti kriterijais grįstą vertinimo metodą saugumo reikalavimų kokybei nustatyti;
3. Taikant pasiūlytą metodą, atlikti techniniuose aprašymuose (specifikacijose) taikytų saugumo reikalavimų eksperimentinį kokybės vertinimą;
4. Apibendrinti gautus rezultatus ir pateikti išvadas.

Planuojamas rezultatas: Tikimasi, kad darbe bus pasiūlytas kriterijais grįstas informacinių sistemų ir/ar registrų IT saugos reikalavimų vertinimo metodas, skirts vertinti jų kokybę. Metodas turi būti išbandytas praktiškai, o gauti rezultatai apibendrinti ir pateiktos išvados.

Vadovas Donatas Vitkus

Vilniaus Gedimino technikos universitetas
Fundamentinių mokslų fakultetas
Informacinių sistemų katedra

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

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

Pavadinimas	**MCDM metodų taikymas registrų ir informacinių sistemų specifikacijų saugumo reikalavimų kokybei vertinti**
Autorius	**Rytis Šakalys**
Vadovas	**Donatas Vitkus**

Kalba: lietuvių

Anotacija

Baigiamajame magistro darbe aprašomas daugiakriterių sprendimo priėmimo metodų pritaikymas registrų ir informacinių sistemų specifikacijų saugumo reikalavimų kokybei vertinti, siekiant šį procesą patobulinti. Užduotis atliekama, pasiūlant daugiakriterį metodą, skirtą saugumo reikalavimų kokybei vertinti. Vertinimas atliekamas, pasitelkus kriterijus, identifikuotus ekspertinės apklausos metu. Pasiūlytame metode yra taikomi AHP, WASPAS ir FUZZY TOPSIS daugiakriteriai metodai. Naudojant AHP metodą buvo gautos kriterijų svertinės reikšmės, o taikant WASPAS ir FUZZY TOPSIS metodus bei remiantis ekspertinės grupės atsakymais, buvo nustatytas registrų ir informacinių sistemų specifikacijose pateiktų saugumo reikalavimų apibrėžties kokybės lygis. Atlikus siūlomo metodo verifikavimo eksperimentą buvo nustatyti aspektai, kuriais siūlomas metodas yra pranašesnis už tradicinį (nestruktūrizuotą) vertinimo metodą.

Darbą sudaro 7 dalys: įvadas, analitinė dalis, siūlomo metodo teorinis aprašymas, siūlomo metodo praktinis taikymas, siūlomo metodo verifikavimo eksperimentas, išvados, literatūros sąrašas.

Darbo apimtis – 69 p. teksto be priedų, 8 iliustr., 43 lent., 31 bibliografinis šaltinis, 8 priedai.

Prasminiai žodžiai: MCDM, daugiakriteriai sprendimo priėmimo metodai, daugiakriteriai metodai, saugumo reikalavimai, registrai ir informacinės sistemos, specifikacijos, techniniai aprašai, kokybės vertinimas, kokybės lygio nustatymas, AHP, WASPAS, FUZZY TOPSIS.

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

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

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

Title	**Application of MCDM Methods to the Quality Assessment of Security Requirements for Registries and Information System Specifications**
Author	**Rytis Šakalys**
Academic supervisor	**Donatas Vitkus**

Thesis language: Lithuanian

Annotation

The final master thesis describes the application of multi-criteria decision-making methods to evaluate the quality of security requirements for registries and information system specifications, with a aim of improving this process. The task is carried out by proposing a multi-criteria approach for evaluating the quality of security requirements. The evaluation is carried out using the criteria identified in an expert questionnaire. The proposed method applies AHP, WASPAS and Fuzzy TOPSIS methods. The AHP method has been used to obtain the weights of the criteria, while the WASPAS and Fuzzy TOPSIS methods, together with the answers of the expert group, have been used to determine the level of quality of the definition of the security requirements for registries and information systems specifications. The verification experiment of the proposed method has identified aspects in which the proposed method is superior to the traditional (unstructured) evaluation method.

The thesis consists of 7 parts: introduction, analytical part, theory of the proposed method, practice of the proposed method, experiment to verify the proposed method, conclusions, literature list.

The volume of the thesis is 69 pages of text without appendices, 8 illustrations, 43 tables, 31 bibliographic sources, 8 appendices.

Keywords: MCDM, multi-criteria decision methods, multicriteria methods, security requirements, registries and information systems, specifications, technical specifications, quality evaluation, quality level determination, AHP, WASPAS, Fuzzy TOPSIS.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

SANTRUMPOS

MCDM (angl. *Multiple Criteria Decision-Making*) – daugiakriteris sprendimų priėmimas

SFR (angl. *Security Functional Requirements*) – funkciniai saugumo reikalavimai

UML (angl. *Unified Modeling Language*) – unifikuota (vieninga) modeliavimo kalba

MADM (angl. *Multiple Attribute Decision-Making*) – daugiakriteris sprendimų priėmimas pagal kelis požymius (atributus)

MODM (angl. *Multiple Objective Decision Making*) – daugiatikslis sprendimų priėmimas

WSM (angl. *Weighted Sum Model*) – daugiakriteris metodas, kuriame taikomas svertinių sumų modelis

WPM (angl. *Weighted Product Model*) – daugiakriteris metodas, kuriame taikomas svertinės sandaugos modelis

TOPSIS (angl. *Technique for Order of Preference by Similarity to Ideal Solution*) – pirmenybių tvarkos technika, veikianti pagal panašumo idealiam sprendimui idėją

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

WASPAS (angl. *Weighted Aggregated Sum Product Assesment*) – svertinės apjungtos sumos multiplikacinis būdas, kuris sudarytas iš WSM ir WPM modelių

Fuzzy TOPSIS – neapibrėžtoms aibėms skirta TOPSIS technika

OWASP (angl. *Open Worldwide Application Security Project*) – pelno nesiekianti bendruomenė, siekianti pagerinti programinės įrangos saugumą

KDR – kraujo donorų registras

MR – mokinių registras

VIPVIS – valstybės informacinių technologijų paslaugų valdymo informacinė sistema

PTR – perleidžiamųjų teisių registras

NTIS – nacionalinė turizmo informacinė sistema

ĮVADAS

Tyrimo aktualumas. Šiuolaikinėje skaitmeninėje aplinkoje registrų ir informacinių sistemų saugumo užtikrinimas yra itin svarbus siekiant apsaugoti jautrią informaciją nuo kibernetinių grėsmių. Vis didėjantis duomenų kiekis ir jų svarba lemia, kad organizacijos turi taikyti aiškius ir efektyvius sistemų saugumo reikalavimus. Tačiau šių reikalavimų kokybė ir tinkamumas gali skirtis nuo įvairių veiksnių, įskaitant teisinius reglamentus, technologinius aspektus bei, be abejo, organizacinius poreikius. Sprendimų priėmimo daugiakriteriai metodai (MCDM) tampa efektyviu būdu vertinant techniniuose aprašuose pristatomų saugumo reikalavimų kokybę. Metodai leidžia sistemingai įvertinti ir palyginti skirtingus saugumo reikalavimų vertinimo kriterijus, alternatyvas bei pristatyti vieningą ekspertinės grupės požiūrį – visa tai padeda objektyviai įvertinti skirtingą reikalavimų apibrėžtį, o kartu ir sudaro sąlygas tolesniam jų tobulinimui. Siūlomo vertinimo metodo taikymas gali prisidėti prie informacinių sistemų patikimumo didinimo, sumažinant galimas saugumo spragas ir didinant atsparumą kibernetinėms atakoms. Taip pat kokybiškai parengtos specifikacijos prisideda prie teisinės ir reguliacinės atitikties užtikrinimo, geresnio išteklių paskirstymo. Taigi baigiamojo darbo tyrimas yra aktualus ir naudingas praktiniam taikymui organizacijose, siekiančiose užtikrinti efektyvią informacijos apsaugą, kuomet ši priklauso nuo specifikuotų saugumo reikalavimų kokybės. Šiame darbe pristatoma, kaip naudojant pasiūlytą kriterijais grįstą vertinimo metodiką yra atliekamas techniniuose aprašymuose (specifikacijose) taikytų saugumo reikalavimų kokybės vertinimas.

Tyrimo problema. Registrų ir informacinių sistemų saugumo reikalavimų kokybė tiesiogiai veikia organizacijų gebėjimą apsisaugoti. Remiantis Nacionaline kibernetinio saugumo strategija, Lietuvos valstybės informaciniai ištekliai tebėra prioritetinis kibernetinio šnipinėjimo taikinys („Lietuvos Respublikos Nacionalinė kibernetinio saugumo strategija“, 2023). Nepaisant didelio dėmesio kibernetiniam saugumui, praktikoje dažnai susiduriama su problemomis, kai specifikacijose pateikti saugumo reikalavimai yra nepakankamai aiškūs, kelia papildomų interpretacijų, yra neišsamūs arba nepritaikyti konkrečiai organizacijai (Mellado ir kt., 2010). Darbe siūlomas vertinimo metodas padės sukurti kokybišką, struktūruotą vertinimo metodą, padėsiantį organizacijoms objektyviai įvertinti specifikacijose apibrėžiamus saugumo reikalavimus ir priimti pagrįstus sprendimus dėl jų tobulinimo. Pasitelkus daugiakriterius metodus, išsamiai įvertinami skirtingi specifikacijų saugumo aspektai, siekiant ne tik laikytis teisinių ir reguliacinių aspektų, bet ir užtikrinti realų, efektyvų saugumą. Toks požiūris padės organizacijoms sustiprinti sistemų atsparumą augančioms grėsmėms.

Tyrimo objektas – registrų ir informacinių sistemų saugumo reikalavimų kokybės vertinimo metodai.

Tyrimo tikslas – patobulinti registro ir informacinės sistemos saugumo reikalavimų kokybės vertinimą, taikant daugiakriterius sprendimo priėmimo metodus.

Uždaviniai tikslui pasiekti:

1. Atlikti registrų ir informacinių sistemų saugumo reikalavimų ir jų kokybės gerinimo analizę, kartu pristatant daugiakriterius metodus;
2. Pasiūlyti kriterijais grįstą vertinimo metodą saugumo reikalavimų kokybei nustatyti;
3. Taikant pasiūlytą metodą, atlikti techniniuose aprašymuose (specifikacijose) taikytų saugumo reikalavimų eksperimentinį kokybės vertinimą;
4. Apibendrinti gautus rezultatus ir pateikti išvadas.

1. REGISTRŲ IR INFORMACINIŲ SISTEMŲ SAUGUMO REIKALAVIMŲ ANALIZĖ

Skyriuje pristatoma registrų ir informacinių sistemų saugumo reikalavimų analizė bei kokybės aspektai. Pristatomi techniniai saugumo reikalavimai (ir funkciniai, ir nefunkciniai). Analizuojama saugumo reikalavimų kokybė, įvardijami reikalavimų atributai bei funkciniai komponentai, pristatoma kokybės lygių klasifikacija. Skyriuje taip pat nagrinėjami daugiakriteriai sprendimų priėmimo metodai, pristatoma jų klasifikacija ir tarpusavio palyginimas. Galiausiai pristatomi apibendrinti mokslinės literatūros analizės rezultatai.

1.1.Registrai ir informacinės sistemos

Registras – informacinėje sistemoje tvarkomas registruojamą objektą ar objektus apibūdinantis duomenų rinkinys ar rinkiniai, kuriems nustatomos specialios registravimo sąlygos („Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas“, 2023). Tai savita duomenų bazė, duomenų rinkinys, kuriam yra nustatomos specialios registravimo sąlygos. Registras yra svarbi duomenų tvarkymo dalis, nes jame yra saugomi visi duomenys, kurie yra reikalingi informacinėms sistemoms veikti. Registrai įprastai yra vieši duomenų rinkiniai, kuriuos tvarko valstybės institucijos. Tačiau registrai yra ne tik duomenų saugyklos, bet ir svarbūs saugumo elementai. Jie gali būti naudojami kaip pirmoji gynybos linija nuo kenkėjiškų atakų, nes prireikus gali blokuoti prieigą prie svarbios informacijos.

Informacinės sistemos, lyginant su registrais, yra žymiai sudėtingesnės struktūros, kurios apima ne tik duomenų bazes, bet ir programinę įrangą, skirtą duomenų tvarkymui ir viešųjų paslaugų teikimui. Saugumo stiprinimo sprendimai, taikomi informacinėse sistemose, gali būti labai įvairūs ir priklauso nuo konkrečios sistemos reikalavimų ir funkcijų.

Užduotys, kurias atlieka registrai ir informacinės sistemos, yra skirtingos, tačiau jų pagrindinis tikslas yra užtikrinti, kad informacija visą laiką būtų saugi, patikima ir prieinama.

Pagrindinės registrų ir informacinių sistemų teikiamos funkcijos šių dienų veiklose:

- duomenų valdymas – padeda organizuoti, saugoti ir valdyti didelius duomenų kiekius;
- procesų efektyvumas – optimizuoja organizacijų veiklą leidžiant valdyti ir apdoroti informaciją;
- sprendimų priėmimas – remiantis aktualia ir tikslia informacija, prisidedama prie geresnių sprendimų priėmimo procesų;
- saugumas – užtikrina duomenų konfidencialumą, vientisumą ir prieinamumą.

Norint geriau suprasti, kaip veikia registrai ir informacinės sistemos, būtina susipažinti su jų techniniais aprašais (specifikacijomis).

1.2.Techniniai aprašai ir saugumo reikalavimai

Registrų ir informacinių sistemų techniniai aprašai (specifikacijos) yra dokumentai, kurie nustato minimalius elektroninės informacijos saugos techninius reikalavimus registrams, informacinėms sistemoms ir kitoms informacinėms sistemoms. Techninė specifikacija – dokumentas, kuriame nustatomi techniniai reikalavimai, kuriuos turi įgyvendinti (išpildyti) gaminys, procesas ar paslauga (International Organization for Standardization, 1999). Minėtų registrų ir informacinių sistemų sauga bei jos įgyvendinimas realioje sistemoje yra implementuojamas naudojant nustatytus saugumo reikalavimus ir kitus sprendimus, kurie įforminami specifikacijoje. Dokumente aprašomas tobulinimo reikalingumas, jam keliami veiklos reikalavimai, kurie apima vidinius ir išorinius duomenų srautus, duomenų modelius bei jų teikimą ir naudojimą, nefunkcinius reikalavimus. Aprašuose pateikto turinio įgyvendinimas padeda apsaugoti duomenis nuo neteisėtos prieigos, jų modifikavimo, sunaikinimo ar kitų grėsmių.

Saugumo reikalavimais yra vadinami reikalavimai, kurie turi tiesioginį poveikį saugiam sistemos veikimui arba užtikrina atitiktį nustatytai saugumo politikai (International Organization for Standardization, 2008). Reikalavimai nustatomi remiantis klientų ir paslaugų tiekėjų tarpusavio susitarimais, tam tikros srities standartais, taikomais teisės aktais, įstatymais ir ankstesnių pažeidžiamumų istorija. Siekiant išspręsti konkrečią saugumo problemą arba likviduoti galimą pažeidžiamumą, saugumo reikalavimuose apibrėžiamos naujos funkcijos arba jau esamų funkcijų papildymai. Vietoj to, kad sukurti kiekvienai taikomajai programai savitą saugumo sprendimą, įprasti saugumo reikalavimai sudaro sąlygas jų kūrėjams pakartotinai naudoti saugumo kontrolės priemones ir geriausias praktikas. Aiškiai, tiksliai ir visoms pusėms gerai suprantami reikalavimai yra esminis sėkmingo projekto įgyvendinimo požymis. Pagrindinė reikalavimų taikymo paskirtis – išvengti saugumo nesėkmių ar jų pasikartojimo.

1.2.1.Funkciniai ir nefunkciniai reikalavimai

Saugumo reikalavimai gali būti skirstom į dvi pagrindines grupes – funkcinius ir nefunkcinius reikalavimus. Funkciniai reikalavimai apibrėžia funkcines galimybes, ką sistema turi daryti, kokias funkcijas ji turi vykdyti ir kaip ji turi veikti (International Organization for Standardization, 2023). Tai konkrečios sistemos funkcijos, kurias ji turi atlikti norint atitikti iškeltus poreikius ir tikslus. Šio tipo reikalavimai gali būti pateikiami formuluojant naudojimo

atvejus arba tiesiogiai aprašant, kokias funkcijas sistema turi turėti, pavyzdžiui - vartotojas turi turėti galimybę prisijungti prie sistemos naudodamas savo vartotojo vardą ir slaptažodį - funkcinis reikalavimas. Kuriant funkcinius reikalavimus programinės įrangos plėtojimo kontekste, labai svarbu vadovautis SMART metodologija, kuri teigia, kad reikalavimai privalo būti konkretūs (angl. specific), pamatuojami (angl. measurable), pasiekiami (angl. achievable), susiję (angl. relevant) ir apibrėžti laike (angl. time-bound). Kitaip tariant, funkciniai reikalavimai turi būti (Visure, s.a.):

- konkrečiai nurodantys, ką sistema turėtų daryti;
- pamatuojami, su tikslu nustatyti, ar sistema atlieka tam tikrą veiksmą;
- pasiekiami per nustatytą laiką;
- susiję su vykdomos veiklos tikslais;
- apibrėžti laiko atžvilgiu progreso kontrolei.

Svarbu suprasti, kad skirtingų sričių (tipų) ar vykdomos veiklos sistemoms gali būti keliami konkretesni funkciniai reikalavimai, kurie gali apimti ne tik vartotojų srautus ar sąveikos scenarijus. Toliau pateikiamas funkcinių ir nefunkcinių reikalavimų savybių palyginimas, pristatantis, kaip ir kokiais aspektais šie reikalavimai tarpusavyje išsiskiria programinės įrangos plėtojimo kontekste (žr. 1 lentelė).

1 lentelė. Funkcinių ir nefunkcinių reikalavimų savybių tarpusavio palyginimas

	Funkciniai reikalavimai	***Nefunkciniai reikalavimai***
Tikslas (siekis)	Apibrėžti, ką sistema atliks	Apibrėžti, kaip sistema veiks
Galutinis rezultatas	Nustatyti sistemos bruožus	Nustatyti sistemos savybes
Pagrindinis dėmesys	Vartotojų reikalavimai	Vartotojų lūkesčiai
Būtinumas	Būtinas	Nebūtinas, tačiau itin pageidaujamas
Kilmė	Įprastai apibrėžiamas iš vartotojo perspektyvos	Apibrėžia programinės įrangos inžinieriai, ekspertai
Dažniausiai naudojami pavyzdžiai	Autentifikacija, autorizacijos lygiai, duomenų apdorojimas, atskaitomybė ir kt.	Tinkamumas naudoti (angl. *usability*), patikimumas, plečiamumas, našumas, atitikimas ir kt.

Šaltinis: sudaryta autoriaus remiantis Altersoft (2023)

Priešingai nei funkciniai reikalavimai, nefunkciniai reikalavimai yra tiesioginiai nesusiję su sistemos funkcionalumu, tačiau jie nustato (apibrėžia) kaip sistema turėtų veikti, kokiu apribojimus ji turi atitikti. Tokio tipo reikalavimai turi patenkinti nustatytus poreikius ir tam tikras sąlygas. Nors nefunkciniai reikalavimai nėra laikomi svarbesniais už funkcinius, tačiau jie išlieka esminiai, siekiant užtikrinti programinės įrangos kokybę, nes jų svarba yra didesnė už pavienių funkcinių reikalavimų svarbą (Pereira ir kt., 2013). Pavyzdžiui, techninėje specifikacijoje elektroninės informacijos saugos priemonių parinkimo principai pagal saugumą ir slaptumą (konfidencialumą) užtikrinančius nefunkcinius reikalavimus gali būti šie:

- turi būti įgyvendinamos tinkamos techninės ir organizacinės priemonės, kad būtų užtikrintas pavojaus lygiui proporcingas saugumas;
- likutinė rizika turi būti sumažinta iki priimtino lygio;
- informacijos saugos priemonės diegimo kaina turi būti adekvati saugomos informacijos vertei;
- pagal situaciją, kur galima, turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

Bent vieno iš nefunkcinių reikalavimų neįvykdymas (neatitikimas jam) gali tapti svaria visos sistemos funkcionavimo sutrikimo priežastimi, o tokių situacijų ištaisymas yra itin brangus pinigine prasme, taip pat taisymas užima daug laiko (Chung & do Prado Leite, 2009).

Dažniausiai implementuojami nefunkciniai reikalavimai su sveikatos priežiūra susijusiose informacinėse sistemose, remiantis mokslinėje literatūroje pateikiamomis išvadomis (Alencar ir kt., 2019):

2 lentelė. Nefunkcinių reikalavimų taikymas (pristatymas) literatūros šaltiniuose

Literatūros šaltinis	***Taikytas (pristatytas) nefunkcinis reikalavimas***
(Michiel Meulendijk ir kt., 2014)	Prieinamumas, sertifikavimas, perkeliamumas, privatumas, saugumas, stabilumas, patikimumas ir tinkamumas naudoti (angl. *usability*)
(Triantafyllidis ir kt., 2015)	Privatumas, saugumas, patikimumas ir efektyvumas, prieinamumas, suderinamumas (angl. *interoperability*), tinkamumas naudoti
(Gómez-Martínez ir kt., 2015)	Tinkamumas naudoti, efektyvumas, plečiamumas
(Blake ir kt., 2016)	Tinkamumas naudoti, patikimumas, plečiamumas, perkeliamumas, saugumas ir privatumas

Literatūros šaltinis	*Taikytas (pristatytas) nefunkcinis reikalavimas*
(Hadjidimitriou ir kt., 2016)	Saugumas ir privatumas, tinkamumas naudoti, tiekimo (pristatymo) (angl. *delivery*) reikalavimai, perkeliamumas

Remiantis analizuotais literatūros moksliniais šaltiniais galima daryti išvadą, kad su sveikatos priežiūra susijusių informacinių sistemų nefunkciniai reikalavimai dažnai persidengia tarpusavyje, sudarydami bendrą visumą. Tarp taikytų (pristatytų) nefunkcinių reikalavimų pagrindiniais elementais išskiriami saugumas ir privatumas – šie reikalavimai minimi didžiojoje dalyje šaltinių. Taip pat tarp dažniausiai minimų nefunkcinių reikalavimų galima išskirti tinkamumą naudoti (angl. *usability*), prieinamumą, perkeliamumą, plečiamumą ir patikimumą.

1.3.Saugumo reikalavimų kokybės vertinimas

Nors mokslinėje literatūroje pakankamai plačiai diskutuojama ir yra įžvelgiama didelė reikalavimų kokybės tyrimų apimtis (terminas „kokybė“ yra pakankamai dažnai minimas), tačiau kokybės tyrimuose daugiausia dėmesio yra skiriama reikalavimų kokybės gerinimo (plėtojimo, tobulinimo, išlaikymo ir kt.) metodams, o kokybės požymių apibrėžimų ir vertinimų tema nagrinėjama tik labai mažoje imtyje pirminių tyrimų (Montgomery ir kt., 2022). Situacija tampa dar labiau kompleksiškesnė, kuomet siekiama išgauti informaciją apie reikalavimų kokybę, susijusią su sistemų saugumu – tokiu atveju yra kliaunamasi tarptautiniuose standartuose sutelktomis gerosiomis praktikomis (International Organization for Standardization, 2022). Toliau pristatomas esminis turinys – mokslinės literatūros šaltinių teikiama informacija apie reikalavimų kokybės atributus (požymius) bei tarptautinių standartų teikiamus funkcinius saugumo komponentus.

1.3.1.Reikalavimų kokybės atributai

Nors esminiu reikalavimų kokybės atributų aspektu yra laikomas tiesioginis jų poveikis projekto sėkmei ar nesėkmei, tačiau atlikti tyrimai rodo, kad aiškūs, išsamūs ir gerai struktūrizuoti reikalavimai yra būtini sėkmingiems projektams įgyvendinti, o dviprasmiški, nenuoseklūs ar nepakankamai apibrėžti reikalavimai dažnai lemia sistemų ar net projektų veikimo nesėkmę. Paprastai tariant, kokybės aspektų indėlis yra esminis, siekiant pagerinti reikalavimų inžinerijos praktiką, o kartu ir sumažinti nesėkmių riziką dėl netinkamai apibrėžtų

(specifikuotų) reikalavimų. Toliau pristatomi kokybės atributų kodai, kuriuos apjungus yra išskiriami atitinkami reikalavimų kokybės atributai (Montgomery ir kt., 2022) (žr. 3 lentelė).

3 lentelė. Reikalavimų kokybės atributų kodai ir klasės

Pavieniai kokybės atributų kodai mokslinės literatūros šaltiniuose	***Kodus apimantys kokybės atributai (klasės)***
Consiceness, granularity, requirement length	*Complexity* (Kompleksiškumas)
Valuable, satisfiability, importance, preference, obsoleteness, negotiability, desirability, creativity	*Relevancy* (Aktualumas)
Use cases, functionality, duplicate activities	*Redundancy* (Pertekliškumas)
Pronoun, non-present tense, NFR, modal verb, negative adjective, compound predicate	*Correctness* (Korektiškumas)
Use of keywords, terminology, step numbering, independent, coverage, coherence	*Consistency* (Nuoseklumas)
Cohesion, interaction, contextual information, individual, conceptual, references	*Completeness* (Išbaigtumas)
Optionality, superlatives, pragmatic, vague, plural, loopholes, lexical, imlicitness	*Ambiguity* (Dviprasmiškumas)
Readability, expressiveness, clarity	*Understandability* (Suprantamumas)
Modifiability, frequency, efficiency	*Reusability* (Pernaudojamumas)

Šaltinis: sudaryta autoriaus remiantis Montgomery ir kt. (2022)

Lentelėje pristatomas turinys perteikia pavienių kokybės atributų kodų skirstymą į kokybės atributų klases. Pavyzdžiui, reikalavimų kokybės atributų klasę (vėlesnėse darbo dalyse vadinamos atributais) *relevancy* (liet. aktualumas) gali sudaryti tokie atributų kodai kaip *valuable* (liet. naudingas), *importance* (liet. svarba), *satisfiability* (liet. patenkinamumas), *preference* (liet. pirmenybė) ir kt. Reikalavimų kokybės atributų klases sudarančių kodų kiekis gali varijuoti, tačiau įprastai didesnis kodų kiekis leidžia lengviau pristatyti situaciją ir apibrėžti vieningą požymių klasę. Remiantis literatūros šaltiniais galima drąsiai teigti, kad išbaigtumas (angl. *completeness*), dviprasmiškumas (angl. *ambiguity*), nuoseklumas (angl. *consistency*) ir korektiškumas (angl. *correctness*) yra pagrindiniai kokybės kriterijai, kuriuos nagrinėja mokslinė literatūra (Heck & Zaidman, 2018; Pekar ir kt., 2014).

1.3.2.Funkciniai saugumo komponentai

Siekiant reikalavimų kokybės atributus susieti su baigiamojo darbo temos specifika, būtina atsižvelgti į svarbiausią – saugumo – pusę. Šiuo atveju, pristatomas ISO/IEC 15408-2:2022 standartas, kurio pirminė paskirtis yra apsaugoti informacijos ir privatumo sritis, taip pat gali būti naudojamas kibernetinio saugumo užtikrinimui. Visgi svarbiausias aspektas apie šį standartą yra tai, kad jis pateikia rekomenduotinas sritis IT saugumo vertinimui, išskiriant jas per funkcinius saugumo komponentus - jame apibrėžtas iš anksto nustatytų funkcinių saugumo reikalavimų (SFR) sąrašas, kurį galima naudoti specifikuojant, projektuojant ir vertinant jau įgyvendintas informacinių sistemų saugumo užtikrinimo priemones. Standarte taip pat pateikiami struktūrizuoti, daugkartinio naudojimo funkciniai komponentai, kuriuos organizacijos gali naudoti siekdamos užtikrinti nuoseklų ir pamatuojamą požiūrį į saugumo reikalavimų apibrėžimą. Taigi ISO/IEC 15408-2 standarto gairės sistemų techniniuose aprašuose padeda nurodyti saugumo reikalavimus taip, kad būtų galima atlikti sistemų vertinimą, siekiant atitikti šių dienų keliamus saugumo poreikius.

Šiame standarte saugumo funkcionalumai yra suskirstyti į modulinę struktūrą, o tai leidžia laisviau pasirinkti, derinti tarpusavyje bei pritaikyti saugumo reikalavimus, atsižvelgiant į konkrečias sistemos saugumo reikmes. Saugumo funkciniai komponentai yra suskirstyti į 11 klasių, iš kurių kiekvienoje yra po keletą reikalavimų šeimų (angl. *families*). Kiekviena klasė atspindi skirtingus saugumo funkcijų aspektus, kuriuos gali tekti spręsti registrui ar IT sistemai. Toliau pateikiama detalesnė informacija apie reikalavimų klases (žr. 4 lentelė).

4 lentelė. Funkcinių saugumo komponentų suskirstymas

Klasės kodas	***Klasės pav.***	***Klasės tikslas***	***Klasės šeimų pav., pvz.,***
FCS	*Cryptographic Support*	Nurodomos kriptografinės operacijos, algoritmai, raktų valdymas	*Cryptographic key management (FCS_CKM), Cryptographic operation (FCS_COP), Random bit generation (FCS_RBG)*
FDP	*User Data Protection*	Nurodo duomenų prieigos kontrolę, konfidencialumo ir vientisumo apsaugą	*Access control policy (FDP_ACC), Access control functions (FDP_ACF), Data authentication (FDP_DAU)*

FIA	*Identification and Authentification*	Apibrėžia naudotojų tapatybės ir autentiškumo patikrinimą	*Authentication proof of identity (FIA_API),* *Authentication failures (FIA_AFL),* *User attribute definition (FIA_ATD)*
FMT	*Security Management*	Apibrėžia administracines saugumo funkcijas, politikų valdymą ir vykdymą	*Limited capabilities and availability (FMT_LIM),* *Management of security attributes (FMT_MSA),* *Security attribute expiration (FMT_SAE)*
FPR	*Privacy*	Apima privatumo kontrolės priemones, skirtas naudotojų duomenų apsaugai	*Anonymity (FPR_ANO),* *Pseudonymity (FPR_PSE).,* *Unlinkability (FPR_UNL)*
FTP	*Trusted path/channels*	Apibrėžia saugius ryšio kanalus, skirtus saugoti perduodamus duomenis	*Trusted channel protocol (FTP_PRO),* *Trusted path (FTP_TRP)*
FRU	*Resource Utilization*	Apibrėžia prieinamumo ir atsparumo gedimams mechanizmus	*Fault tolerance (FRU_FLT),* *Priority of service (FRU_PRS),* *Resource allocation (FRU_RSA)*
FTA	*Target of Evaluation (TOE) Access*	Nurodo sistemos prieigos kontrolę, įskaitant ir sesijų valdymą	*Limitation on scope of selectable attributes (FTA_LSA),* *Session locking and termination (FTA_SSL),* *TOE access banners (FTA_TAB)*
FPT	*Protection of the TSF*	Apibrėžia sistemos vientisumą, saugų ryšį ir apsaugą nuo klastojimo	*TOE emanation (FPT_EMS),* *Fail secure (FPT_FLS),* *Availability of exported TSF data (FPT_ITA)*

FAU	*Security Audit*	Nustatomi įvykių registravimo, stebėjimo ir audito mechanizmai	*Security audit automatic response (FAU_ARP),* *Security audit data generation (FAU_GEN),* *Security audit analysis (FAU_SAA)*
FCO	*Communication*	Nurodomi neatšaukiamumo ir saugaus ryšio mechanizmai	*Non-repudiation of origin (FCO_NRO),* *Non-repudiation of receipt (FCO_NRR)*

Lentelėje pristatyta informacija savaime nėra reikalavimų kokybę pristatantis turinys, tačiau tai ypatingai pasitarnaus tolesnėje šio darbo eigoje, kuomet bus stengiamasi suformuoti pirminių vertinimo kriterijų sąrašą, apimant tiek reikalavimų kokybės atributus, tiek saugumo aspektus, taip siekiant patobulinti registrų ir informacinių sistemų specifikacijose pateiktų saugumo reikalavimų kokybės vertinimą.

1.3.3.Kokybės lygių klasifikacija

Siekiant objektyviai ir nuosekliai įvertinti saugumo reikalavimų kokybę bei lengviau palyginti alternatyvas, vertinimas grindžiamas trimis kokybės lygiais: tinkamu, patenkinamu ir koreguotinu. Šie lygiai leidžia ekspertiškai įvertinti, kiek saugumo reikalavimų rinkinys (scenarijus) atitinka esminius kokybės atributus, tokius kaip išsamumas, aiškumas, nuoseklumas, korektiškumas ir aktualumas ir t.t. Toks klasifikavimas kokybės prasme padeda ne tik išryškinti stipriąsias ar silpnąsias alternatyvas, bet ir orientuoja į tolesnes jų tobulinimo kryptis. Detalesnė informacija pateikiama toliau (žr. 5 lentelė).

5 lentelė. Saugumo reikalavimų kokybės lygių klasifikacija

Kokybės lygio pavadinimas	***Kokybės lygį apibrėžiančios skaitinės reikšmės***	***Kokybės lygio apibrėžimas (apibūdinimas)***
Tinkamas lygis	$Q \geq 0.90$ $C_i \geq 0.90$	Reikalavimų rinkinys (scenarijus) laikomas tinkamo lygio ir jo apibrėžtis atitinka arba beveik atitinka išsamumo, aiškumo, nuoseklumo, korektiškumo,

Kokybės lygio pavadinimas	*Kokybės lygį apibrėžiančios skaitinės reikšmės*	*Kokybės lygio apibrėžimas (apibūdinimas)*
		aktualumo ir kitus kokybės atributus
Patenkinamas lygis	$0.70 \leq Q < 0.90$ $0.70 \leq C_i < 0.90$	Reikalavimų rinkinys (scenarijus) laikomas atitinkančiu minimalų kokybės lygį, tačiau gali pasitaikyti ne esminių trūkumų, kurie susiję su apibrėžties ne išsamumu, nuoseklumo trūkumu
Koreguotinas lygis	$Q < 0.70$ $C_i < 0.70$	Reikalavimų rinkinys (scenarijus) yra laikomas žemiau toleruotinos (patenkinamos) ribos, jis vargiai atitinka keliamus kokybės poreikius – įžvelgiami detalumo, specifiškumo (tikslumo) trūkumai, kyla interpretacijų apibrėžtyje

Lygių klasifikavimas leidžia sistemingai ir kritiškai įvertinti saugumo reikalavimų rinkinių kokybinį atitikimą. Aiškiai apibrėžti kokybės lygiai – tai ne tik vertinimą apibendrinanti priemonė, bet ir praktinis pagrindas kokybiškesnių, geriau valdomų saugumo reikalavimų vystymui.

1.4.Daugiakriteriai sprendimų priėmimo metodai

Šiandieniniame pasaulyje sprendimų priėmėjai susiduria su įvairialypiais iššūkiais, kuriems įveikti reikia struktūruoto ir pagrįsto požiūrio (Sahoo & Goswami, 2023). Daugiakriteriai metodai itin aktualūs iki šios dienos - konkrečių atvejų analizėse aptariami įvairūs tyrimai, kuriuose MCDM buvo naudojami tokiose srityse kaip pagalba priimant medicininius sprendimus, taip pat ekonominiuose bei finansiniuose aspektuose (Alamoodi ir kt., 2023). Šiame poskyryje apžvelgiamos skirtingos MCDM metodikos, jų klasifikacija. Pateikiamas skirtingų metodų tarpusavio palyginimas, privalumai ir trūkumai.

1.4.1. Daugiakriterių sprendimo priėmimo metodų sąvoka ir klasifikacija

Daugiakriterių sprendimų priėmimo (angl. *Multiple Criteria Decision-Making*, MCDM) metodai siūlo sistemingą struktūrą sprendimų problemoms, susijusioms su keliais tikslais, įvairiais kriterijais ir skirtingais pageidavimais, spręsti (Ananda & Herath, 2009). Tai vienas iš pagrindinių sprendimų priėmimo procesų, kuriuo siekiama nustatyti geriausią įmanomą alternatyvą atsižvelgiant į daugiau nei vieną atrankos kriterijų (Taherdoost & Madanchian, 2023). Procesas aprėpia daug kriterijų ir kitų, galutiniam sprendimo priėmimui svarbių, veiksnių, pvz., alternatyvų identifikavimą ir įvertinimą, jiems priskiriant svorius ir lyginant juos tarpusavyje.

Yra daugybė MCDM metodų, pasižyminčių skirtingomis savybėmis, kurios gali būti susijusios su bent keletu aspektų, pradedant nuo atsakymų kokybės ir baigiant ties problemos, kurią šie metodai siekia spręsti, tipu. Todėl norint geriau suprasti MCDM metodikas, būtina nustatyti klasifikaciją. Tiesa, svarbu paminėti ir tai, kad skirtinguose tyrimuose yra pripažįstamos ir šiek tiek skirtingos klasifikacijos, tačiau taip yra dėl atskiro atsižvelgimo į skirtingus problemų niuansus.

Mokslinėje literatūroje pateikiama bent keletą būdų, kaip klasifikuoti daugiakriterius metodus (Taherdoost & Madanchian, 2023). MCDM yra skirstomi į 2 pagrindines grupes:

- Kelių atributų (daugiaatributis) sprendimų priėmimo metodas (angl. *Multi Attribute Decision Making*, MADM) – metodas, iš konkrečių žinomų alternatyvų sąrašo išsirenkama racionaliausia alternatyva (Simanavičienė, 2011). Dar vadinamas kaip diskrečiųjų problemų sprendimu ir yra sutelktas į problemas su aiškiai žinomomis sprendimo alternatyvomis, kurių skaičius yra baigtinis;
- Kelių objektų/tikslų (daugiaobjektis arba daugiatikslis) sprendimų priėmimo metodas (angl. *Multi Objective Decision Making*, MODM) – vektorinės optimizacijos procesą naudojantis metodas, kuris grįstas sprendimo proceso modeliu (Simanavičienė, 2011). Šis metodas dar yra skaidomas į kelias sub-kategorijas naudojamų alternatyvų klasifikavimui pagal pradinius duomenis:
    - Neapibrėžtų aibių (angl. *fuzzy*);
    - Stochastiniai (arba tikimybiniai);
    - Deterministiniai.

1.4.2.Daugiakriterių sprendimo priėmimo metodų apžvalga ir palyginimas

Egzistuoja bent kelios dešimtys skirtingų daugiakriterių sprendimų priėmimo metodų, tačiau literatūroje išskiriami ir vieni dažniausiai naudojamų metodų yra šie (Kolios ir kt., 2016):

- WSM (angl. *Weighted Sum Model*) arba dar kitaip literatūroje vadinamas SAW (angl. *Simple Additive Weighting*) – paprasčiausias ir dažniausiai naudojamas svorių sudėjimo metodas, kuris teigia, kad kiekvienos alternatyvos vertė yra lygi bendrai jų sumai;
- TOPSIS (angl. *Technique for Order of Preference by Similarity to Ideal Solution*) metodas grįstas idėja, kad geriausia įmanoma alternatyva yra kuo arčiau idealaus sprendimo ir kartu kuo toliau nuo neidealaus sprendimo;
- WPM (angl. *Weighted Product Model*) – analogiškas sprendimas WSM metodui, tačiau šis metodas vietoje svorių sudėties naudoja sandaugą.
- AHP (angl. *Analytic Hierarchy Process*) metodas, kurio tikslas nustatyti optimalią alternatyvą ir suskirstyti kitas, atsižvelgiant į jas apibūdinančius kriterijus;
- ELECTE (pranc. *Elimination Et Choix Traduisant la Realité* – „Eliminavimas ir pasirinkimas verčiant tikrovę“) – metodas skirtas pasirinkimo, rūšiavimo ir reitingavimo problemoms spręsti, leidžiantis pasirinkti geriausią alternatyvą iš sąrašo;
- PROMETHEE (angl. *Preference Ranking Organization Method for Enrichment Evaluation*) prioritetinis metodas, kuris atlieka porinį alternatyvų palyginimą apskaičiuodamas išeinančių ir įeinančių alternatyvų vertes (Wang ir kt., 2016)
- WASPAS (angl. *Weighted Aggregated Sum Product Assesment*) – svertinės apjungtos sumos multiplikacinis būdas, kuris sudarytas iš WSM ir WPM (angl. *Weighted Product Model*) (Zavadskas ir kt., 2012a);
- MAUT (angl. *Multi Attribute Utility Theory*) prioritetinis metodas, kuris optimaliausią sprendimą priima pagrindžiant naudingumo apskaičiavimais;
- SMART (angl. *Simple-Multi Attibute Rating Technique*) – metodas, kuris naudoja paprastesnę MAUT tipo versiją (Mark Velasquez & Patrick Thomas Hester, 2013);
- Fuzzy TOPSIS – TOPSIS metodo taikymas neapibrėžtoje aplinkoje (Mokhtarian, 2015);

Pateikti metodai yra skirtingi, todėl lyginti juos tarpusavyje yra gana sudėtinga. Dažnu atveju metodai skiriasi savo kompleksiškumu, taikymu, subjektyvumu ir kt. – dėl šių trūkumų

objektyvus palyginimas (įvertinimas) neįmanomas. Daugumą pristatytų metodų apima toliau pateikiama lyginamoji lentelė (Poškas ir kt., 2012) (žr. 6 lentelė).

6 lentelė. Daugiakriterių sprendimų priėmimo metodų palyginimas

Savybė	***AHP***	***Fuzzy***	***WSM***	***WPM***	***ELECTRE PROMETHEE***	***TOPSIS***	***MAUT***
Pasaulinė praktika inž. MCDA uždav. spręsti	+	±	-	-	±	±	±
Grupinis sprendimų priėmimas	±	+	+	+	±	±	±
Tiesinė uždavinio struktūra	-	+	+	+	+	+	+
Hierarchinė uždavinio struktūra	+	-	-	-	-	-	-
Įverčių suderinamumo užtikrinimas	+	-	-	-	+	+	+
Kokybinių kriterijų įvertinimas	+	+	-	-	+	+	+
Skirtingos kriterijų matavimo dimensijos	+	+	-	+	+	+	+
Metodo suprantamumas	Vidutinis	Vidutinis	Paprastas	Paprastas	Sudėtingas	Sudėtingas	Sudėtingas
Darbo sąnaudos	Vidutinės	Vidutinės	Mažos	Mažos	Didelės	Didelės	Didelės

Kiekvieno lentelėje (žr. 6 lentelė) pateikto metodo atitiktis nustatytoms savybėms yra skirtinga. Apibendrinus pateiktus duomenis galima teigti, kad šio darbo tikslui pasiekti tinkamiausias savybes atitinka AHP, WSM, WPM ir Fuzzy daugiakriteriai sprendimų priėmimo metodai.

Toliau pateikiama detalesnė anksčiau pateiktų sprendimo metodų apžvalga (žr. 7 lentelė). Joje pristatomi metodų privalumai, trūkumai, panaudojimo sritys (Mark Velasquez & Patrick Thomas Hester, 2013; Sahoo & Goswami, 2023; Siksnelyte-Butkiene ir kt., 2020):

7 lentelė. Detalesnė MCDM apžvalga

Metodas	*Panaudojimo sritys*	*Privalumai*	*Trūkumai*
WSM, WPM, SAW	Visur, kur prireikia spręsti itin paprastas sprendimų priėmimo problemas; verslas ir finansai	Lengvai suprantamas bei pritaikomas; paprastas skaičiavimas; intuityvumas	Rezultatai gali būti nelogiški; daro prielaidą, kad kriterijai yra vienodai svarbūs
TOPSIS	Inžinerija, logistika, gamyba, gamtosauga, verslas ir marketingas, žmogiškieji resursai	Lengvai suprantamas, aiškus ir intuityvus; leidžia atsižvelgti į teigiamus ir neigiamus kriterijų aspektus, atsižvelgti į kompromisus ir priešingus tikslus; laikomas stabiliausiu metodu, esant nepastoviems duomenims; net esant dideliam duomenų kiekiui, išlaiko tokį patį, problemai spręsti reikalingų žingsnių kiekį	Jautrus duomenims - esant skirtumams tarp alternatyvių sprendimų, galutinis rezultatas gali būti netikslus; neatsižvelgia į sprendimo duomenų neapibrėžtumą ar netikslumą
AHP	Efektyvumo problemoms spręsti; resursų planavimui; kur reikia - spręsti sudėtingas sprendimų priėmimo problemas	Leidžia išskaidyti sudėtingas problemas į kriterijų ir alternatyvų hierarchiją	Skaičiavimai užima daug laiko; labai priklauso nuo porinio palyginimo tikslumo ir nuoseklumo, kuris gali būti subjektyvus ir veikiamas individualių šališkumų
ELECTRE	Energetikos, aplinkosaugos, ekonomikos problemų sprendimui	Leidžia atsižvelgti į daugybę kriterijų su skirtingais svarbos lygiais; taikoma peržengimo sąvoka, pagal kurią atsižvelgiama ne į absoliučius balus, o į santykinius alternatyvų rezultatus; gali apdoroti netikslius ir neapibrėžtus duomenis	Gali generuoti nesuderinamus rezultatus, kai alternatyvų rangavimas nėra nuoseklus ar logiškas; veiklos ribos ir pirmenybės parametrai yra subjektyvūs ir reikalauja kruopštaus kalibravimo; būti netinkamas didelės apimties sprendimų problemoms spręsti
PROMETHEE	Gamyba, energetika, logistika, verslas ir finansai	Lankstus alternatyvų, su konfliktuojančiais kriterijais, reitingavimas ir palyginimas; leidžia sprendimų priėmėjams įtraukti skirtingas pirmumo funkcijas ir kriterijų svorius; siūlo grafinius vaizdus	Daro prielaidą, kad kriterijai yra nepriklausomi, ir aiškiai neįvertina kriterijų sąveikos ar priklausomybės; jautriai reaguoja į pirminių parametrų pokyčius
MAUT	Energetika, ekonomika, finansai, agrokultūra	Galima naudoti netikslius duomenis, kai trūksta informacijos; gali apdoroti ir kokybinius, ir kiekybinius kriterijus	Daug resursų reikalaujantis procesas; reikalauja daug duomenų; išreikšti pageidavimai turi būti labai tikslūs
GRA	Verslas, vadyba	Atsižvelgia į neapibrėžtumą taikant tikimybinius modelius ir sprendimų analizės metodus; mažiau jautrus nukrypimams ir kraštutinėms reikšmėms	Daro prielaidą, kad tarp kriterijų ir jų veiksmingumo yra tiesinis ryšys; gali netinkamai atspindėti sudėtingus sprendimų priėmimo scenarijus, kai tarp kriterijų egzistuoja netiesiniai ryšiai arba sąveika
WASPAS	Verslas, logistika, žmogiškieji ištekliai	Leidžia svarstyti ir teigiamus ir neigiamus alternatyvų niuansus; lengvas skaičiavimo procesas	Reikalauja duomenų normalizavimo; įvertinamos tol minimalios ir maksimalios alternatyvų reikšmės

Metodas	*Panaudojimo sritys*	*Privalumai*	*Trūkumai*
Fuzzy TOPSIS	Finansai, vadyba, medicina, gamtosauga, inžinerija	Trūkstant informacijos, leidžia naudoti netikslius duomenis; leidžia sprendimų priėmėjams tvarkyti neaiškumus ir neapibrėžtumą sprendimo duomenyse; apima ir teigiamus, ir neigiamus kriterijų aspektus	Sunkiai suprantamas; reikia apibrėžti lingvistinius kintamuosius; daro prielaidą, kad tarp kriterijų ir jų efektyvumo yra tiesinis ryšys

Siekiant išspręsti konkrečią problemą, privalu pasirinkti tinkamiausią metodą jai. Būtina įsitikinti keliamos problemos ir metodo tarpusavio veikimo suderinamumu. Pasirinkus teisingą metodą bei sėkmingai jį pritaikius keliamai problemai, įprastai, galutinis rezultatas pasižymės tikslumu, patikimumu bei teisingumu.

1.5.Analitinės dalies išvados

Šiame skyriuje buvo pristatyta registrų ir informacinių sistemų saugumo reikalavimų analizė, ji susidarė iš esminių terminų ir apibrėžimų, funkcinių ir nefunkcinių reikalavimų analizės, saugumo reikalavimų kokybės klasifikacijos pristatymo bei daugiakriterių sprendimų priėmimo metodų apžvalgos.

Remiantis moksline literatūros analize bei surinktais atskirų analizių, aprašymų ir apžvalgų duomenimis, suformuojamos išvados:

1. Saugumo reikalavimai turi tiesioginį poveikį saugiam sistemos veikimui. Šie reikalavimai įprastai yra skirstomi į funkcinius ir nefunkcinius. Funkciniai reikalavimai apibrėžia, ką sistema atliks, nefunkciniai – kaip sistema veiks. Dažniausiai išskiriami nefunkciniai reikalavimai sveikatos priežiūros informacinėse sistemose yra saugumas ir privatumas;
2. Didžiojoje mokslinių kokybės tyrimų dalyje vyrauja reikalavimų kokybės gerinimo metodai, o kokybės požymių, vertinimų bei apibrėžimų temos yra nagrinėjamos ganėtinai retai. Tokie reikalavimų kokybės atributai kaip aiškumas, išsamumas, korektiškumas yra būtini sėkmingų projektų įgyvendinimui. Reikalavimų kokybės atributų susiejimas su ISO/IEC 15408-2:2022 standarto funkciniais saugumo komponentais suteikia galimybę modeliuoti specifinius saugumo reikalavimų kokybės vertinimo kriterijus;
3. Tinkamas daugiakriterių sprendimų priėmimo metodų (MCDM) pasirinkimas yra itin svarbus. Norint užtikrinti gaunamų rezultatų patikimumą, reikia įsigilinti ne tik į užduoties problematiką, ypatybes ir duomenis, tačiau ir į asmens, priimančio sprendimus, tikslus, galimybes (žinių ir įgūdžių aspektus),

pageidavimus. Esminiu patampa ir pasirinktas metodas – idealaus ir visiems atvejams tinkančio varianto nėra, todėl itin patartina atkreipti dėmesį į metodo taikymo sritį, teikiamus privalumus ir trūkumus.

2. KRITERIJAIS GRĮSTO LYGINAMOJO VERTINIMO METODAS

Šioje dalyje apibūdinamas vertinimo metodas, taikomas sprendžiant registrų ir informacinių sistemų specifikacijose apibrėžtų saugumo reikalavimų kokybės problemą, taikant daugiakriterius sprendimų priėmimo metodus. Saugumo reikalavimai techniniuose aprašuose ne visada atitinka aukščiausius kokybės lūkesčius, pvz., jie nėra išbaigiami iki galo, pateikiami nekorektiškai. Šios ir panašios situacijos sukuria kokybės gerinimo poreikį. Toliau pateikiama metodika leis išnaudoti daugiakriterių sprendimo priėmimo metodus (MCDM), siekiant likviduoti vyraujančias problemas.

2.1.Kriterijais grįsto lyginamojo vertinimo apibūdinimas

Kriterijai yra esminiai elementai lyginamajame vertinime. Jie apibrėžia svarbiausius aspektus ir (ar) reikalavimus, pagal kuriuos bus vertinami ir palyginami skirtingi variantai ar alternatyvos. Šie kriterijai, priklausomai nuo esamos situacijos ir specifinių poreikių gali varijuoti, tačiau tikslingai (teisingai) apibrėžti kriterijai sutaupo ne tik laiko, bet kartu užtikrina vertinimo proceso efektyvumą ir objektyvumą. Kadangi šis darbas orientuotas į registrų ir informacinių sistemų saugumo reikalavimų kokybės vertinimo pagerinimą, pasiūlant daugiakriterį vertinimo metodą, identifikuoti kriterijai privalo būti tiesiogiai susiję saugumo reikalavimų svarbiausiais aspektais.

2.2.Saugumo reikalavimų kriterijų sąrašo sudarymas

Prieš pradedant taikyti anksčiau apžvelgtus daugiakriterius sprendimų priėmimo metodus, privaloma sudaryti saugumo reikalavimų kriterijų sąrašą. Šis sąrašas sudaromas remiantis mokslinėje literatūroje pateikiama informacija, ISO/IEC 15408 standartu bei kitais objektyviais šaltiniais (International Organization for Standardization, 2022; Montgomery ir kt., 2022). Vėlesnėje darbo eigoje, sudarytas sąrašas pateikiamas ekspertinei grupei vertinimui, siekiant išgauti, jų nuomone, daugiausiai įtakos saugumo reikalavimų kokybei turinčius 5 kriterijus. Kadangi sprendžiamos problemos sprendimui nustatyti privaloma pasirinkti keletą reikšmių, pateikiamas platesnis 12 kriterijų sąrašas (žr. 8 lentelė).

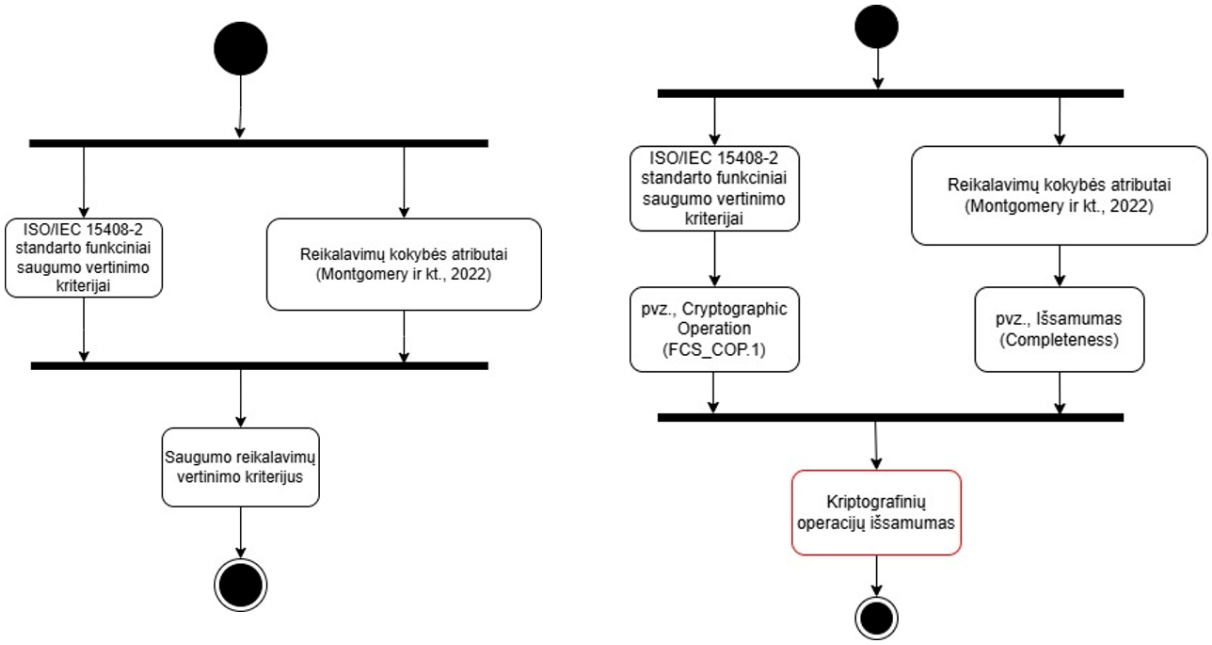
8 lentelė. Kriterijų sąrašas reikalavimams vertinti

Vertinimo kriterijaus pavadinimas	***Kriterijaus kokybės atributas***	***Kriterijaus apibūdinimas, pvz.,***
Kriptografijos palaikymo išsamumas	Išsamumas – reikalavimas turi pakankamai apimti aspektus, kuriems jis yra skirtas	Ar nurodyta, kokie kriptografiniai algoritmai turi būti naudojami (pvz., AES, RSA)?

Vertinimo kriterijaus pavadinimas	*Kriterijaus kokybės atributas*	*Kriterijaus apibūdinimas, pvz.,*
		Ar nurodyta, kaip šifravimo raktai yra saugomi ir valdomi? (pvz., HSM) Ar nurodytas atitikimas pasaulyje pripažintiems kriptografiniams standartams (pvz., ISO/IEC 19790)?
Vartotojų identifikacijos ir autentifikacijos aktualumas	Aktualumas – reikalavimas turi būti aktualus taikomai sistemai ir atitikti jos numatytus poreikius	Ar yra apibrėžtas autentifikavimo mechanizmas (pvz., slaptažodis, biometrika, PIN, 2FA)? Ar autentifikacijos duomenys yra apsaugoti nuo atakų (pvz., hashing, salt)?
Sistemos architektūros integracijos išsamumas	Išsamumas – reikalavimas turi pakankamai apimti aspektus, kuriems jis yra skirtas	Ar reikalavime nurodyti visi esminiai architektūros sluoksniai (pvz., duomenų, veiklos logikos, vartotojo sąsajos, saugumo), būtini sklandžiai integracijai? Ar nurodyta, kaip architektūra palaikys augimą, keičiamumą ir suderinamumą su būsimais sistemos ar infrastruktūros pokyčiais?
Papildomų saugumo priemonių korektiškumas	Korektiškumas – reikalavimas turi būti techniškai ir logiškai pagrįstas, neprieštarauti saugumo normoms ar standartams	Ar siūloma saugumo priemonė techniškai įgyvendinama turimoje sistemos architektūroje ir ar jos naudojimas pagrįstas konkrečiais grėsmių scenarijais?
Saugumo įvykių registravimo nepertekliškumas	Nepertekliškumas – reikalavimas neturi kartoti kitų specifikacijoje apibrėžtų punktų ar įtraukti nereikalingų, nereikšmingų elementų	Ar reikalavime išdėstyta informacija nedubliuoja kitų saugumo įvykių registravimo reikalavimų specifikacijoje? Ar registravimo priemonės ir tvarka nėra perteklinės ar nereikalingai sudėtingos lyginant su tikslu ir teikiama praktine nauda?
Atitikimo tarptautiniams standartams nedviprasmiškumas	Nedviprasmiškumas – reikalavimas turi būti formuluojamas taip, kad jį būtų galima interpretuoti tik vienu būdu	Ar reikalavime nedviprasmiškai nurodytas konkretus standartas (pvz., ISO/IEC 27001:2013) ir taikoma jo dalis, o ne bendra nuoroda „laikytis standartų“? Ar reikalavimo formuluotė leidžia tik vieną galimą interpretaciją dėl standartų taikymo apimties, sričių ar atsakomybės?
Atkūrimo po saugumo sutrikimų išbaigtumas	Išbaigtumas – reikalavimas turi turėti visas būtinas sudedamąsias dalis	Ar yra įdiegtos automatinės atkūrimo priemonės gedimo atvejais?

Vertinimo kriterijaus pavadinimas	*Kriterijaus kokybės atributas*	*Kriterijaus apibūdinimas, pvz.,*
		Ar apibrėžti atkūrimo po saugumo sutrikimų reikalavimai turi visas būtinas sudedamąsias dalis?
Atsparumo prieinamumo išpuoliams nepertekliškumas	Nepertekliškumas – reikalavimas neturi kartoti kitų specifikacijoje apibrėžtų punktų ar įtraukti nereikalingų, nereikšmingų elementų	Ar reikalavimas apsiriboja tik esminiais, būtinais komponentais ir mechanizmais, kurie tiesiogiai prisideda prie sistemos atsparumo DDoS ar kitokiems prieinamumo trikdžiams? Ar reikalavime pateikta informacija proporcinga rizikai, t. y. ar nėra perteklinių sprendimų, kurių kaštai ar sudėtingumas neadekvatūs realiai grėsmei?
Prieigos kontrolės politikos nuoseklumas	Nuoseklumas - reikalavimas turi derėti su kitais sistemos saugumo reikalavimais ir būti integruotas	Ar apibrėžti prieigos kontrolės reikalavimai yra pakankamai integruoti (ar dera bendrame saugumo kontekste)? Ar prieigos kontrolės politikos taisyklės yra taikomos visiems vartotojams, įskaitant ir administratorius?
Atitikties teisinei ir reguliacinei sistemai išsamumas	Išsamumas - reikalavimas turi pakankamai apimti aspektus, kuriems jis yra skirtas	Ar apibrėžti nacionaliniai (tarptautiniai) teisiniai bei reguliaciniai reikalavimai pakankamai apima aspektus, kuriems yra skirti?
Saugos priemonių parinkimo principų korektiškumas	Korektiškumas - reikalavimas turi būti techniškai ir logiškai pagrįstas, neprieštarauti saugumo normoms ar standartams	Ar yra paisoma diegiamų saugos priemonių kainos ir saugomos informacijos vertės adekvatumo?
Duomenų konfidencialumo užtikrinimo aiškumas	Aiškumas - reikalavimas yra suformuluotas tiksliai, vengiant abstrakčių ar neaiškių terminų	Ar duomenų konfidencialumo užtikrinimas yra apibrėžtas vengiant abstrakčių ir neaiškių terminų? Ar apibrėžti kontrolės mechanizmai nėra abstraktūs ir pernelyg lakoniški?

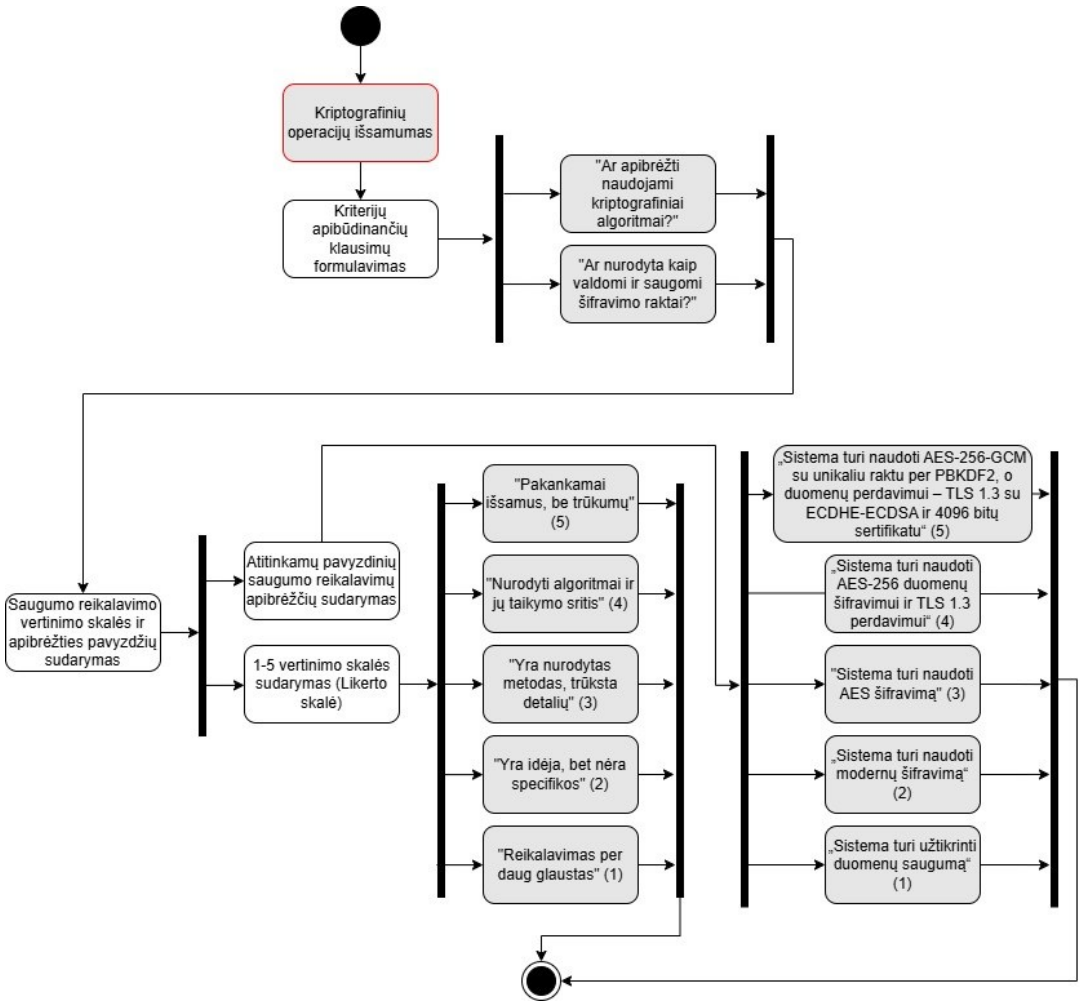
Techniniuose aprašuose pateikiamų saugumo reikalavimų kokybei nustatyti būtina sudaryti tinkamus vertinimo kriterijus. Tai atliekama agreguojant specifinius ISO/IEC 15408 standarte pateikiamus funkcinius saugumo vertinimo kriterijus ir mokslinėje literatūroje pateikiamus reikalavimų kokybės atributus (papildoma informacija pristatoma 1.3.1. ir 1.3.2. skyreliuose). Detalesnė informacija pateikiama UML veiksmų diagramos pavidalu (žr. 1 pav.).



1 pav. Saugumo reikalavimų vertinimo kriterijaus sudarymas - aiškinamoji bendrinė schema (kairėje) ir aiškinamoji pavyzdinė schema (dešinėje)

Šaltinis: sudaryta autoriaus

Sudarius pirminį kriterijų sąrašą bei pristačius kriterijų sudarymo konceptą, taip pat svarbu pristatyti ir pavyzdinę vertinimo metodiką – t. y. pavyzdys, kuriuo ekspertai galės vadovautis ekspertinio vertinimo metu, siekiant įvertinti registrų ir informacinių sistemų specifikacijose pateiktų saugumo reikalavimų kokybę. Pavyzdys susidaro iš 2 esminių dalių – vertinimo skalės (Likerto skalė) bei vertinamų reikalavimų apibrėžties pavyzdžių (žr. 2 pav.).



2 pav. Saugumo reikalavimų vertinimo skalės ir pavyzdinių reikalavimų sudarymo aiškinamoji schema (naudojamas „Kriptografijos palaikymo išsamumas“ kriterijus)

Šaltinis: sudaryta autoriaus

Kaip pristatoma schemoje, atitinkamas techninio aprašo reikalavimas gali būti įvertinamas tam tikra, eksperto nuomonę atspindinčia, skaitine reikšme. Pilka spalva pažymėti langeliai laikomi kintančiais nuo specifinio kriterijaus pobūdžio.

Kai jau yra žinomas saugumo reikalavimų kriterijų sąrašas, kitas žingsnis yra nustatyti jiems skaitines svorių reikšmes, t. y. nustatyti, kriterijų reikšmingumą. Kriterijų svorių reikšmes (svarbą) įvertina ekspertų grupės dalyviai. Ši skaitinė reikšmė tolimesniame procese atspindės kriterijų svarbą priimant tam tikrus sprendimus.

2.3.Ekspertų grupės sudarymas

Siekiant užtikrinti vertinimo tikslumą, objektyvumą, profesionalumą ekspertų grupės dalyviai turės praeiti atrankos procesą, kurio metu bus įvertinamas jų atitikimas iškeltiems kriterijams, siejamiems su jų turimais įgūdžiais, sukauptomis žiniomis, darbo patirtimi, kompetencijomis. Atrankos procese naudojami bent keli skirtingi būdai išgryninti dalyvius:

anketų užpildymas, individualiai pritaikyti vertinimo metodai bei kolektyvinis vertinimas (Ginevičius ir kt., 2009). Atrankos procesas leidžia ne tik įvertinti dalyvių atitikimą, tačiau kartu kelia didesnį patikimumo (saugumo) jausmą ekspertų atsakymų prasme, o tai sąlygojasi su galutinių rezultatų kokybe ir tikslumu.

Ekspertų komandos atrankos proceso vykdymas pradedamas nuo kriterijų, kuriems dalyviai turi atitikti, apibrėžimo. Kaip jau minėta, viena iš svarbiausių savybių, kuriai skiriamas didžiausiais dėmesys yra eksperto (dalyvio) kompetencija. Kompetencijai įrodyti įprastai gali užtekti mokslų baigimo diplomų, papildomų išklausytų kursų diplomų ar sertifikatų. Tačiau labai dažnai pasitaikanti sąlyga ekspertų atrankos procese yra ne tik jų turima kompetencija, o ir straipsnių, vadovėlių, knygų ar kito tipo publikacijų išleidimas eksperto veikimo srityje (NLP asociacija, 2014). Deja, tačiau galimybių įvertinti ekspertų kompetenciją šiuo metu nėra, todėl pretenduojančius dalyvius bus siekiama įvertinti remiantis keliais esminiais kriterijais:

- Įgytas tiksliųjų mokslų pakraipos bent bakalauro laipsnis;
- Darbo patirtis IT srityje arba darbo patirties saugumo reikalavimų inžinieriaus, sistemų auditoriaus, ar kitoje, su sistemų plėtojimu bei reikalavimais susijusioje pozicijoje;
- Bazinės žinios apie saugumo reikalavimus, jų tipus;
- Analitiškumas, kritinis vertinimas, situacijos vertinimas.

Nors daugelis mokslininkų sutaria, kad kaip minimalų ekspertų grupės dydį turėtų sudaryti bent 3 ekspertai, rekomenduotiną grupės dydį mokslininkai apibrėžia ties 8–10 ekspertų (NLP asociacija, 2014).

2.4.Daugiakriterių sprendimo priėmimo metodų taikymas reikalavimų vertinime

Šiame poskyryje bus pristatomas šio baigiamojo darbo užduoties sprendimas – kriterijais grįstas lyginamojo vertinimo metodas. Toliau bus aprašomi keli metodai – AHP, WASPAS ir „Fuzzy“ TOPSIS. Kriterijų svoriams nustatyti bus naudojami AHP bei „Fuzzy“ TOPSIS metodai. Šiuo atveju, AHP metodas yra skirtas kompleksinėms problemoms spręsti, nes itin gelbėja tais atvejais, kai sprendžiant užduotį tenka naudoti tiek kokybinius, tiek kiekybinius dydžius. Kaip ir buvo kalbėta analitinėje dalyje, šis metodas taip pat suskirsto problemą į savitą hierarchiją, dėl ko didinamas atsakymo tikslumas, išvengiama klaidingų sprendimų priėmimo. Tolesnėje darbo eigoje su AHP ir Fuzzy TOPSIS gauti rezultatai bus naudojami WASPAS ir „Fuzzy“ TOPSIS metodų skaičiavimams pritaikyti.

Nepriklausomai nuo naudojamo daugiakriterio sprendimo priėmimo metodo, visų problemų sprendimas susideda iš šių žingsnių (Simanavičienė, 2011):

1. Pirmas žingsnis – nagrinėjamų alternatyvų vektoriaus sudarymas, iš kurių bus išrenkama racionali alternatyva:

$$A = (A1, A2, \dots, Ai, \dots, Am) \quad (1)$$

2. Antrasis žingsnis – suformuojamas rodiklių, pagal kuriuos vertinamos alternatyvos, vektorius:

$$X = (X1, X2, \dots, Xj, \dots, Xn) \quad (20)$$

Kriterijų sąrašas, kuris bus naudojamas baigiamajame darbe, bus atliktas tik po ekspertinės grupės dalyvių tinkamumo vertinimo pagal anksčiau pristatytą metodiką.

3. Trečiasis žingsnis – sprendimo priėmimo matricos formavimas. Ši matrica yra užpildoma jau kiekybiniais duomenimis, kurie gaunami ekspertiniais (arba statistiniais) duomenimis:

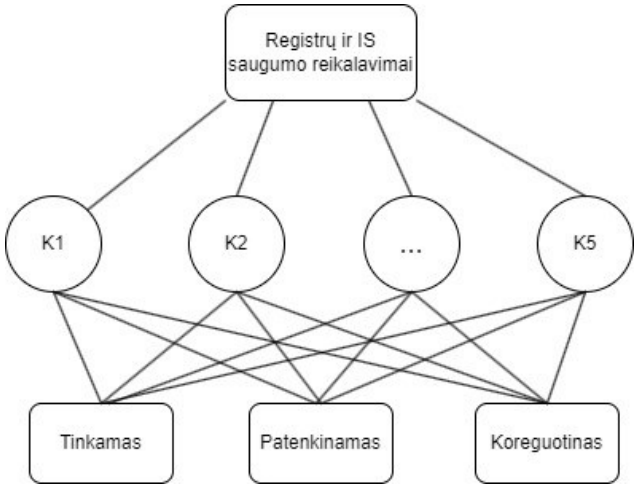
$$X_{|m\times n|} = \begin{pmatrix} X_{11}\ X_{12} \cdots X_{1n} \\ \dots \quad \dots \quad \cdots \quad \dots \\ X_{m1} X_{m2} \cdots X_{mn} \end{pmatrix} \quad (3)$$

Čia taikomi ekspertinio vertinimo duomenys, kadangi nagrinėjamoje problemoje vyrauja kokybiniai kriterijai.

4. Ketvirtasis žingsnis – AHP metodo taikymas siekiant nustatyti kriterijų svorius. Vėliau seks gautų rezultatų perkėlimas WASPAS skaičiavimams atlikti.

5. Penktasis žingsnis - problemos sprendimas TOPSIS metodu.

Pateikiama uždavinio struktūros diagrama (žr. 3 pav.).



3 pav. Užduoties hierarchinė struktūra

2.5.Kriterijų svorio nustatymas

Sprendimų priėmimo procese yra tik dalis MCDM metodų, kurie padeda nustatyti kriterijų vertes (svorius), vienas jų – AHP. Kaip buvo minėta dar daugiakriterių metodų lyginimo metu, šis metodas skaido keliamas problemas į hierarchinę struktūrą, todėl supaprastinamas procesas. Kitas metodas yra TOPSIS. Šis metodas grįstas idėja, kad geriausia įmanoma alternatyva yra kuo arčiau idealaus sprendimo ir kartu kuo toliau nuo neidealaus sprendimo (Kolios ir kt., 2016). Nors TOPSIS dažniausiai yra naudojamas alternatyvų reitingavimui, tačiau jis tai pat gali būti naudojamas ir kriterijų reikšmių nustatymui, kada kriterijai vertinami per alternatyvų reitingavimo prizmę. Tinkamo metodo pasirinkimas leis supaprasti procesą bei paversti jį kaip įmanoma objektyvesniu.

Kriterijų svorio nustatymas naudojantis AHP metodu:

1. Pirmasis žingsnis – 2.4. poskyryje prie antrojo žingsnio pateiktas rodiklių vektoriaus sudarymas:

$$X = (X1, X2, \dots, Xj, \dots, Xn) \qquad (4)$$

Šiuo atveju, kriterijų sąrašas bus patikslintas po atlikto ekspertinio vertinimo.

2. Antrasis žingsnis – ekspertų nustatytų rodiklių (kriterijų) reikšmingumo įvedimas į matricą. Joje bus atliekamas įvestų reikšmių porinis palyginimas (žr. 9 lentelė) (Poškas et al., 2012):

9 lentelė. Porinės koreliacijos matrica

Kriterijai	***K1***	***K2***	***K3***	***...***	***Kn***
K1	1	pp12	pp13	...	pp1n
K2	pp21	1	pp23	...	pp2n
K3	pp31	pp32	1	...	pp3n
...	...	...	...	...	...
Kn	ppn1	ppn2	ppn3	...	1

Porinis palyginimas yra metodas, kuomet kriterijai ir kriterijų alternatyvos yra lyginami siekiant nustatyti, kuris yra svarbesnis. Svarbu paminėti, kad K1, K2, K3 ir sekančios reikšmės simbolizuoja skirtingus kriterijus.

Kriterijų skaitinės vertės yra apsprendžiamos metodika, kuri nurodo, kiek svarbus yra eilutės kriterijus, lyginant su stulpelio kriterijumi. Pavyzdžiui, jeigu K1 yra 3 kartus svarbesnis už K2, reiškiasi pp12 langelio vertė yra 3. Tuo tarpu priešingas langelis pp21 bus skaičiuojamas pagal metodiką pp21=1/pp12, kas yra lygu 0,33 (nes 1/3). Remiantis tokia metodika yra suskaičiuojamos visos lentelės (matricos) langelių vertės. Po matricos užpildymo seka pateiktų duomenų normalizacija (kada susumuojamos visos vienoje eilutėje esančios reikšmės ir vėliau

jau kiekvieną langelio reikšmė dalinama iš to skaičiaus individualiai), šis veiksmas padeda išsigryninti galutinį kiekvieno iš kriterijų svorį. Vėliau ekspertai turi pasinaudoti kriterijų porinio palyginimo skale, norint įvertinti kriterijus. Ši skalė pateikiama toliau (žr. 10 lentelė).

10 lentelė. AHP porinės koreliacijos skalė

Skalė (reitingas)	***Reitingavimo paaiškinimas***
1	Kriterijų svarba yra vienoda (lygi)
3	Kriterijaus pranašumas lyginant su alternatyva - vidutinis
5	Kriterijaus pranašumas lyginant su alternatyva – stiprus
7	Kriterijaus pranašumas lyginant su alternatyva – labai stiprus
9	Kriterijaus pranašumas lyginant su alternatyva – absoliutus
2, 4, 6, 8	Kompromisinės tarpinės reikšmės tarp dviejų gretimų sprendimų
Atvirkštinių reikšmių skalė (reitingas)	***Reitingavimo paaiškinimas***
1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 1/9	Atvirkštinis (priešingas) vertinimas. Jei *i* kriterijus buvo įvertintas *j* kriterijaus atžvilgiu iš aukščiau pateikiamo sąrašo, tuomet *j* kriterijui bus priskiriama atvirkštinė *i* reikšmė

Kaip jau buvo minėta, ši metodologija yra skirta sukurti porinio palyginimo matricai, dėl ko duomenys yra pertvarkomi siekiant išgauti jau galutines kriterijų reikšmes. Norint supaprastinti AHP skaičiavimus, naudojamas *Excel* programos skaičiuoklė-šablonas, kurį sukūrė *SCB Associates*. Šio skaičiavimo šablono rezultatai bus naudojami tolesnėje darbo eigoje.

2.6.WASPAS metodo naudojimo aprašymas

2012 metais sukurtas metodas skaitomas kaip vienas iš naujausių tarp daugiakriterių sprendimų priėmimo metodų šeimos (Badalpur & Nurbakhsh, 2021). Šis metodas yra laikomas sąlyginai jautrus kriterijų svorių ir reikšmių pokyčiams, o tai gali svarbu, kai siekiama įvertinti, kaip net minimalūs kriterijų duomenų pokyčiai keičia sprendimo rezultatą. Metodas susidaro iš toliau pateikiamų žingsnių sekos (Chakraborty & Zavadskas, 2014):

1. Pirmasis žingsnis – 3.3 poskyryje pateiktas sprendimo priėmimo matricos formavimas:

$$X_{|m\times n|} = \begin{pmatrix} X_{11} & X_{12} & \cdots & X_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ X_{m1} & X_{m2} & \cdots & X_{mn} \end{pmatrix} \quad (5)$$

Kai *m* yra alternatyvų skaičius ir *n* yra vertinimo kriterijų skaičius; *xij* yra *i*-osios alternatyvos našumas *j*-ojo kriterijaus atžvilgiu. Reikalavimų vertinimas vykdomas naudojant kokybinius kriterijus, todėl ekspertinis vertinimas privalomas, jame bus taikomos lingvistinės sąvokos, dar vėliau jos bus transformuojamos į skaitines reikšmes. Pertransformavimas vykdomas pagal toliau pateiktą lentelę (žr. 11 lentelė):

11 lentelė. Kiekybinių reikšmių priskyrimas lingvistiniams terminams

Lingvistinis terminas (reikšmingumas)	***Skaitinė maksimali reikšmė***	***Skaitinė minimali reikšmė***
Labai žemas (LŽ)	1	9
Žemas (Ž)	3	7
Vidutinis (V)	5	5
Aukštas (A)	7	3
Labai aukštas (LA)	9	1

2. Antrasis žingsnis – normalizacijos taikymas, naudojant formules:

Normalizacija naudingam kriterijui:

$$\underset{x_{ij}}{\rightarrow} = \frac{x_{ij}}{max_{ij}x_{ij}} \tag{6}$$

Ir nenaudingam kriterijui:

$$\underset{x_{ij}}{\rightarrow} = \frac{min_{ij}x_{ij}}{x_{ij}} \tag{7}$$

čia X_{ij} jau yra normalizuota vertė.

3. Trečiasis žingsnis - naudojantis formulėmis iš WPM ir WSM metodų, ieškomas bendras optimalumo kriterijus remiantis dviem optimalumo kriterijais:

$$Q_i^{(1)} = \sum_{j=1}^{n} \overline{x_{ij}}\, w_j \tag{8}$$

Iš čia w_j yra – j-ojo kriterijaus svoris, nustatytas po AHP skaičiavimų:

$$Q_i^{(2)} = \prod_{j=1}^{n} \left(x_{ij}\right)^{wj} \tag{9}$$

4. Ketvirtasis žingsnis - agreguojamas apibendrintas optimalumo kriterijus pagal toliau pateikimą formulę:

$$Q_i = 0.5Q_i^{(1)} + 0.5Q_i^{(2)} = 0.5\sum_{j=1}^{n} \overline{x_{ij}}\, w_j + 0.5\prod_{j=1}^{n} \left(x_{ij}\right)^{wj} \tag{10}$$

5. Penktasis žingsnis - didesniam reitingavimo tikslumui ir proceso efektyvumui pasiekti, naudojama apibendrinta lygtis i-osios alternatyvos bendrai santykinei svarbai nustatyti, pridedant λ dydį (Zavadskas ir kt., 2012b):

$$Q_i = \lambda Q_i^{(1)} + (1-\lambda) Q_i^{(2)} = \lambda \sum_{j=1}^{n} \overline{x_{ij}}\, w_j + (1-\lambda) \prod_{j=1}^{n} \left(x_{ij}\right)^{wj}, \lambda = 0, 0.1, \dots, 1. \quad (11)$$

6. Šeštasis žingsnis - optimalus λ verčių apskaičiavimas atliekamas naudojant formulę:

$$\lambda = \frac{\sigma^2\left(Q_i^{(2)}\right)}{\sigma^2\left(Q_i^{(1)}\right) + \sigma^2\left(Q_i^{(2)}\right)} \quad (12)$$

7. Septintasis žingsnis - dispersijų apskaičiavimas atliekamas naudojant formules:

$$\sigma^2\left(Q_i^{(1)}\right) = \sum_{j=1}^{n} w_j^2 \sigma^2\left(\overline{x_{ij}}\right) \quad (13)$$

$$\sigma^2\left(Q_i^{(1)}\right) = \sum_{j=1}^{n} \left(\frac{\prod_{j=1}^{n} (x)^{w_j} w_j}{(x_{ij})^{w_j} (x_{ij})^{(1-w_j)}} \right)^2 \sigma^2(x_{ij}) \quad (14)$$

Galiausiai pritaikius visas formules gaunama reikšmė Q, ji – pagrindinis sprendimo priėmimo kriterijus.

2.7.„Fuzzy“ TOPSIS metodo naudojimo aprašymas

Pradinis TOPSIS metodas yra skirtas problemų sprendimui aiškiai apibrėžtoje aplinkoje, kai vyrauja kiekybiniai dydžiai. Neapibrėžtoje aplinkoje yra naudojamas Fuzzy TOPSIS metodas, kuris specialiai tam ir buvo sukurtas - stabilus ir sąlyginai atsparus metodas, kuris leidžia priimti nuoseklius sprendimus esant didesniems svorių pokyčiams apibrėžtumo stokojančioje aplinkoje. Prieš skaičiavimų atlikimą, svarbu kriterijams priskirti kiekybines skaitines reikšmes (žr. 12 lentelė) (Salimov, 2023):

12 lentelė. Lingvistinių reikšmių konvertavimas į skaitines reikšmes

Lingvistinis terminas (reikšmingumas)	***Skaitinės vertės alternatyvoms***	***Skaitinės vertės kriterijams***
Labai žemas (LŽ)	(1,1,3)	(0.1,0.1,0.3)
Žemas (Ž)	(1,3,5)	(0.1,0.3,0.5)
Vidutinis (V)	(3,5,7)	(0.3,0.5,0.7)
Aukštas (A)	(5,7,9)	(0.5,0.7,0.9)
Labai aukštas (LA)	(7,9,9)	(0.7,0.9,0.9)

Metodo naudojimas perteikiamas šiais žingsniais (Dymova ir kt., 2013):

1. Kaip ir kiekvieną kartą pradedant vykdyti MCDM metodą, pradžioje sudaroma sprendimo matrica:

$$X_{|m\times n|} = \begin{pmatrix} X_{11}\, X_{12} \cdots X_{1n} \\ \cdots \quad \cdots \quad \cdots \quad \cdots \\ X_{m1} X_{m2} \cdots X_{mn} \end{pmatrix} \tag{15}$$

2. Antras žingsnis – ekspertų įvertinimų apjungimas:

$$a_{ij} = \min_k \{a_{ij}^k\}, b_{ij} = \frac{1}{K}\sum_{k=1}^{K} b_{ij}^k, c_{ij} = \max_k \{c_{ij}^k\} \tag{16}$$

3. Normalizuotos sprendimų matricos apskaičiavimas vykdomas su šia formule:

$$r_{ij} = \left(\frac{a_{ij}}{c_j^*}, \frac{b_{ij}}{c_j^*}, \frac{c_{ij}}{c_j^*}\right), kur\ c_j^* \equiv \min_i \{c_{ij}\} \tag{17}$$

4. Nustatomos dvi esminės vertės: A*, kuri bus ideali vertė ir A-, kuri bus blogiausia (labiausiai neideali) vertė. Apibrėžiamos formulės:

$$A^* = (\tilde{v}_1^*, \tilde{v}_2^*, \ldots, \tilde{v}_n^*), kur\ \tilde{v}_j^* = \max_i \{v_{ij3}\} \tag{18}$$

$$A^- = (\tilde{v}_1^-, \tilde{v}_2^-, \ldots, \tilde{v}_n^-), kur\ \tilde{v}_j^- = \min_i \{v_{ij1}\} \tag{19}$$

5. Apskaičiuojamas tolis tarp A^* ir A^- verčių:

$$d_i^* = \sum_{(j-1)}^{n} d(\tilde{v}_{ij}, \tilde{v}_j^*) \tag{20}$$

$$d_i^- = \sum_{(j-1)}^{n} d(\tilde{v}_{ij}, \tilde{v}_j^-) \tag{21}$$

6. Apskaičiuojamas artumo koeficientas, kurį žymi C_i:

$$C_i = \frac{D_i^-}{D_i^+ + D_i^-} = (0 \le C_i \le 1; i = 1,2, \ldots, n) \tag{22}$$

2.8.Ekspertų nuomonių suderinamumo vertinimas

Ekspertinio vertinimo patikimumą apie sprendžiamą problemą galima gauti tik įvertinus ekspertų nuomonių suderinamumą, kuris apskaičiuojamas pasitelkiant Kendallio konkordancijos koeficientą W (Kendall, 1990). Šis skaičiavimo metodas leidžia nustatyti, kiek ekspertų vertinimo rezultatai yra suderinti tarpusavyje, siekiant užtikrinti jų tikslumą. Jei ekspertų vertinimai prieštaringi (nesuderinami arba sunkiai suderinami), tada reikšmė W→0,

jei ekspertų vertinimai panašūs - W→1. Apkreiptinas dėmesys, kad itin didelio tikslumo reikalaujančiose srityse tai gali būti kertiniu procesu, nes tam tikro sprendimo priėmimas gali kardinaliai pakeisti sekančių įvykių seką.

Kaip minėta, konkordancijos koeficiento rodiklio *w* reikšmė privalo būti [0, 1] intervale. Tačiau remiantis mokslinėje literatūroje pateikiama informacija, šio rodiklio reikšmės gali būti sėkmingai skirstomos į pakopas, siekiant rezultatus lengviau interpretuoti. Šis skirstymas į pakopas yra pristatomas toliau (Moslem ir kt., 2019) (žr. 13 lentelė).

13 lentelė. Konkordancijos koeficiento rodiklio w skirstymas į pakopas

W rodiklio reikšmė	***Reikšmės apibūdinimas (interpretavimas)***
0	Nėra bendro sutarimo (angl. *no agreement*)
0.10	Silpnas sutarimas (angl. *weak agreement*)
0.30	Vidutinis sutarimas (angl. *moderate agreement*)
0.60	Stiprus sutarimas (angl. *strong agreement*)
1	Visiškas (puikus) sutarimas (angl. *perfect agreement*)

Šaltinis: sudaryta autoriaus remiantis Moslem ir kt. (2019)

Ekspertų nuomonių suderinamumo vertinimo apskaičiavimo žingsniai yra šie (Andriusaitiene ir kt., 2008):

1. Iš pradžių įvertinama kiekvienos alternatyvos reikšmių suma:

$$e_i = \sum_{j=1}^{r} r_{ij} \, (i = 1, \dots, m) \tag{23}$$

   Iš čia – e_i yra reikšmių suma, kuri buvo suteikta ekspertų, r – dalyvavusių ekspertų skaičius, r_{ij} yra ekspeto įvertinta alternatyva *i.*

2. Toliau yra atliekami skaičiavimai, siekiant gauti reikšmių vidurkį:

$$\bar{e} = \frac{1}{n} \sum_{i=1}^{n} e_i \tag{24}$$

   Iš čia – n yra alternatyvų skaičius.

3. Kitas žingsnis – nukrypimo nuo bendro vidurkio apskaičiavimas:

$$S = \sum_{i=1}^{m} (e_i - \bar{e})^2 \tag{25}$$

4. Galiausiai, W vertės (koeficiento) apskaičiavimas naudojant formulę:

$$w = \frac{12 * S}{r^2 m(m^2 - 1)} \tag{26}$$

$$W = \frac{12 * S}{m * n(n+1)} \quad (27)$$

Kuo W reikšmė yra toliau nuo vieneto, tuo pasiektas suderinamumas yra vertinamas prasčiau, ir atvirkščiai – kuo W reikšmė yra toliau nuo nulio, tuo pasiektas suderinamumas yra geresnis

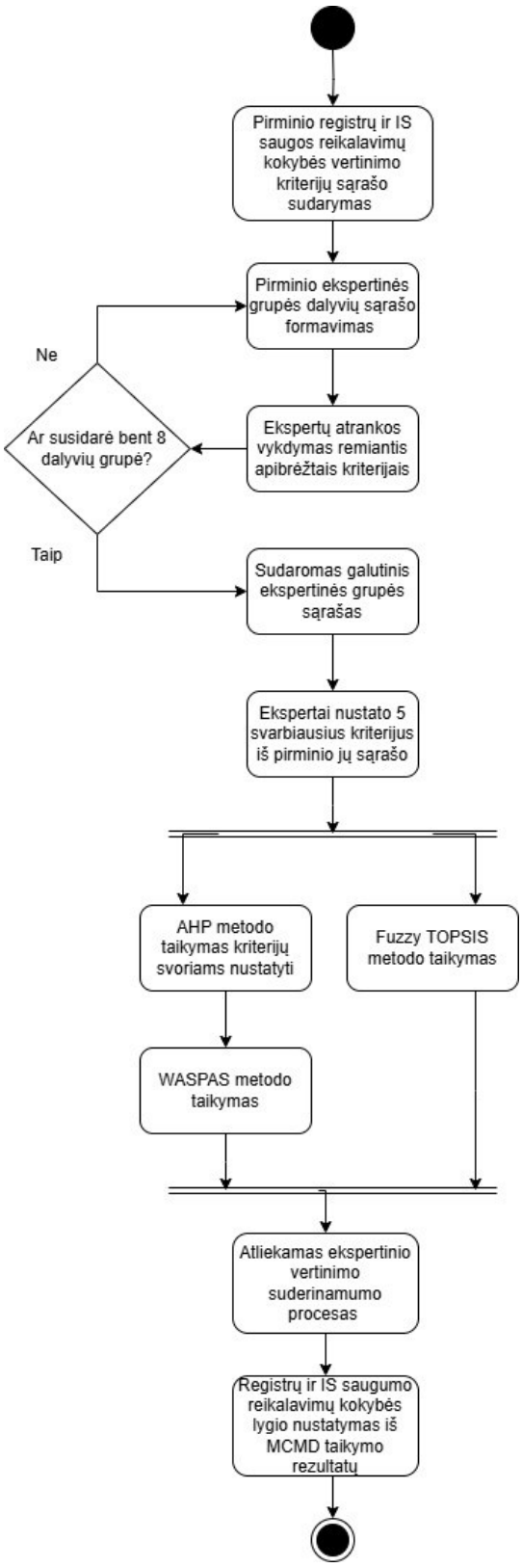
5. Konkordancijos koeficiento reikšmingumas apskaičiuojamas, naudojant formulę:

$$\mathcal{X}^2 = Wr(m-1) = \frac{12 * S}{rm(m+1)} \quad (28)$$

Iš čia, x^2 - chi kvadrato skirstinio reikšmė.

Chi kvadrato laisvės laipsnių skaičius yra lygus v =m-1. Remiantis pasirinkta reikšmingumo verte α, gali būti nustatyta kritinė reikšmė x_{kr}^2. Jeigu ši vertė nėra didesnė už x^2 vertę, matoma, kad atskiros ekspertų nuomones tarpusavyje yra suderinamos (Andriušaitienė, et al., 2008). Tačiau jeigu ekspertų nuomonės yra nesuderinamos, tolimesnis procesas (kriterijų rūšiavimas) yra nebeatliekamas – tokiu būdu siekiama neiškreipti rezultatų susidūrus su duomenų išskirtimis.

Darbo problemai išspręsti naudojama metodika pristatoma toliau (žr. 4 pav.). Diagrama procesą pristato pažingsniui ir padeda suprasti kiekvieno etapo indėlį galutiniam rezultatui pasiekti.



4 pav. Darbo problemos sprendimo metodikos veiksmų diagrama

3. SIŪLOMO DAUGIAKRITERIO METODO EKSPERIMENTINIS VERTINIMAS

Skyriuje pateikiamas anksčiau pristatytų MCDM metodų praktinis taikymas registrų ir informacinių sistemų specifikacijų saugumo reikalavimų kokybės nustatymo procese. Metodo realizavimas vykdomas remiantis ekspertinio vertinimo metu surinktais duomenimis, galiausiai, šie duomenys yra naudojami skaičiavimams atlikti bei galutinėms išvadoms pagrįsti. Skyriuje taip pat pateikiama reliatyvi informacija – ekspertinės grupės atrankos procesas, saugumo reikalavimų rinkinių kokybės reitingo nustatymas, ekspertų tarpusavio nuomonių suderinamumo vertinimas, naudotų metodų jautrumo analizė.

3.1.Ekspertinės grupės atranka

Ekspertinio vertinimo metodas pradedamas nuo pradinio respondentų (ekspertų) sąrašo sudarymo. Sąrašo sudarymas atliekamas vadovaujantis anksčiau pristatytais įtraukimo kriterijais 2.3. poskyryje, kurie apima kandidato įgytą išsilavinimą, darbo patirtį, bazines IT saugumo žinias bei svarbias asmenines savybes. Pradinio ekspertų sąrašo sudarymas pasitarnauja kaip papildomas filtras galutinio respondentų sąrašo sudarymui, tokiu būdu siekiama išvengti potencialaus tarpusavio rezultatų nesuderinamumo bei išskirti stipriausius atrankoje dalyvaujančius ekspertus. Kadangi minimalus rekomenduojamas ekspertų grupės dydis susidaro iš 3 ekspertų, o optimalus – nuo 8 iki 10, siekiama suburti bent 8 ekspertų grupę. Ekspertų paieškos procesui pagreitinti nuspręsta respondentų ieškoti ne tik socialiniame tinkle „LinkedIn“ bet ir kliautis antros pakopos IT saugos studijų studentų nuomonėmis.

3.2.Ekspertinio vertinimo procesas

Pasibaigus galutinės ekspertinės grupės formavimui, toliau pradedamas ekspertinio vertinimo proceso vykdymas. Šis žingsnis yra neatsiejama metodo realizavimo dalis. Pradžioje ekspertai yra supažindinami su tyrimu ir jį supančiomis aplinkybėmis, taip siekiant juos greičiau įvesti į kontekstą apie planuojamus darbus, procesus bei nepalikti vietos interpretacijoms. Kuomet ekspertams nebekyla klausimų apie tolesnę darbo eigą, ekspertams yra perduodamos apklausos formos. Šios formos užpildomos. Iš užpildytų apklausos formų gauti duomenys bus naudojami vėlesniuose tyrimo eigos etapuose.

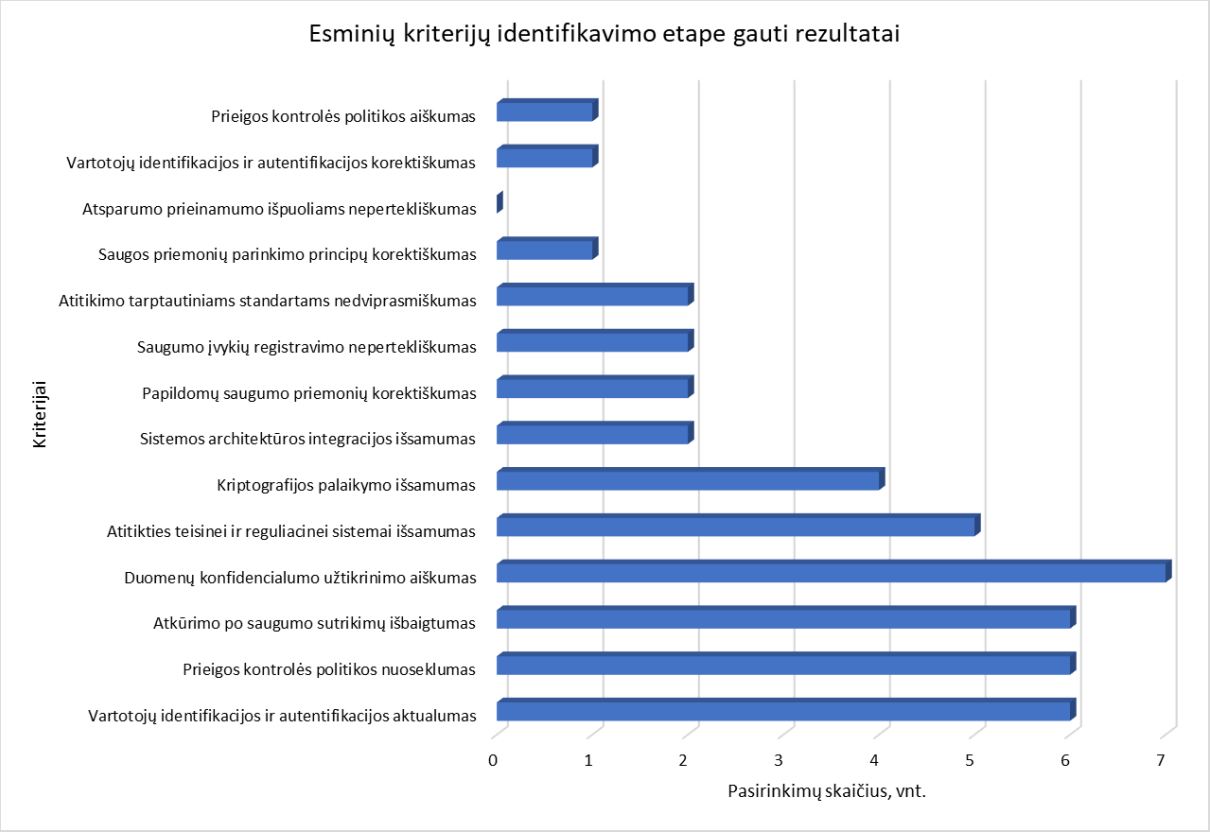
3.2.1.Esminių kriterijų identifikavimas

Esminių kriterijų identifikavimas pradedamas nuo apklausos formos perdavimo eksperimentiniame vertinime dalyvaujantiems respondentams (žr. 1 priedas). Iš šios formos kiekvienas iš ekspertų privalo pasirinkti (išskirti) penkis, jų manymu, svarbiausius kriterijus (ekspertams taip pat paliekama galimybė pasiūlyti, jų manymu, tinkamą kriterijų). 1 priede pateikiamo kriterijų sąrašo gale yra minimi ekspertų pasiūlyti kriterijai. Priedo kriterijų sąrašas (neskaitant proceso metu ekspertų pasiūlytų kriterijų) yra identiškas ankstesnėje darbo dalyje pristatytam sąrašui (žr. 8 lentelė).

14 lentelė. Esminių kriterijų identifikavimo metu gauti rezultatai

Eksperto Nr.	***Eksperto atsakymas***
E1	c), d), g), j), l)
E2	a), b), c), e), k)
E3	f), g), i), j), l)
E4	b), g), i), j), l)
E5	a), b), g), i), l)
E6	a), b), i), j), l)
E7	b), f), g), i), l)
E8	a), b), d), e), n)
E9	g), i), j), l), m)

Grafiškai pristatomi apibendrinti pirmosios (kriterijų identifikavimo) ekspertų apklausos rezultatai (žr. 5 pav.).



5 pav. Esminių kriterijų identifikavimo etape gauti rezultatai

Kaip matoma iš pristatytų apklausos rezultatų, ekspertų asmeninės nuomonės šiek tiek išsiskyrė. Penki, dažniausiai ekspertų pasirinkti kriterijai buvo šie: vartotojų identifikacijos ir autentifikacijos aktualumas, prieigos kontrolės politikos nuoseklumas, atkūrimo po saugumo sutrikimų išbaigtumas, duomenų konfidencialumo užtikrinimo aiškumas bei atitikties teisinei ir reguliacinei sistemai išsamumas. Pora ekspertų pasinaudojo galimybe pasiūlyti, jų nuomone, tinkamus vertinimo kriterijus, kurių pradiniame sąraše nebuvo – prieigos kontrolės politikos aiškumą bei vartotojų identifikacijos ir autentifikacijos korektiškumą, tačiau šie kriterijai didesnio palaikymo tarp ekspertų nesulaukė. Esminių kriterijų identifikavimo etape dalyvavo 9 ekspertai.

Remiantis ekspertų atsakymais buvo išskirti penki svarbiausi kriterijai, nustatant registro ir informacinės sistemos techninio aprašo saugumo reikalavimų kokybę. Ekspertų pateikti atsakymai bus naudojami toliau plėtojant šį darbą.

3.2.2.Kriterijų svorių nustatymas

Esminių kriterijų identifikavimo žingsnyje ekspertams išskyrus svarbiausius kriterijus, šiame žingsnyje siekiama nustatyti svorius išskirtiems kriterijams. Nustatymo procesas yra atliekamas naudojantis AHP metodika, kuri pateikiama šio darbo 2.5. poskyryje. Kaip ir identifikavimo etape, kriterijų svorių nustatymui atlikti bus naudojamas ekspertinis vertinimas

– apklausa (žr. 2 priedas). Proceso metu skaitinės svorių reikšmės bus nustatomos lyginant kriterijus tarpusavyje, išsirenkant svarbiausią. Šios apklausos rezultatai yra pateikiami toliau matricoje (žr. 6 pav.).

E1	K1	K2	K3	K4	K5
K1	1.00	3.00	0.33	0.14	0.33
K2	0.33	1.00	0.33	0.33	0.50
K3	3.00	3.00	1.00	0.33	1.00
K4	7.00	3.00	3.00	1.00	3.00
K5	3.00	2.00	1.00	0.33	1.00

E2	K1	K2	K3	K4	K5
K1	1.00	7.00	5.00	0.33	1.00
K2	0.14	1.00	3.00	1.00	0.20
K3	0.20	0.33	1.00	0.33	1.00
K4	3.00	1.00	3.00	1.00	0.33
K5	1.00	5.00	1.00	3.00	1.00

E3	K1	K2	K3	K4	K5
K1	1.00	0.20	3.00	0.11	5.00
K2	5.00	1.00	1.00	0.20	5.00
K3	0.33	1.00	1.00	1.00	3.00
K4	9.00	5.00	1.00	1.00	3.00
K5	0.20	0.20	0.33	0.33	1.00

E4	K1	K2	K3	K4	K5
K1	1.00	0.33	5.00	7.00	0.33
K2	3.00	1.00	5.00	7.00	0.33
K3	0.20	0.20	1.00	5.00	0.33
K4	0.14	0.14	0.20	1.00	0.20
K5	3.00	3.00	3.00	5.00	1.00

E5	K1	K2	K3	K4	K5
K1	1.00	5.00	0.14	0.20	0.33
K2	0.20	1.00	0.20	0.33	0.33
K3	7.00	5.00	1.00	5.00	7.00
K4	5.00	3.00	0.20	1.00	0.33
K5	3.00	3.00	0.14	3.00	1.00

E6	K1	K2	K3	K4	K5
K1	1.00	3.00	0.33	3.00	5.00
K2	0.33	1.00	0.20	0.20	0.33
K3	3.00	5.00	1.00	0.25	5.00
K4	0.33	5.00	4.00	1.00	3.00
K5	0.20	3.00	0.20	0.33	1.00

E7	K1	K2	K3	K4	K5
K1	1.00	5.00	7.00	5.00	0.33
K2	0.20	1.00	0.20	3.00	0.20
K3	0.14	5.00	1.00	5.00	7.00
K4	0.20	0.33	0.20	1.00	0.33
K5	3.00	5.00	0.14	3.00	1.00

E8	K1	K2	K3	K4	K5
K1	1.00	0.33	5.00	7.00	5.00
K2	3.00	1.00	0.20	0.33	7.00
K3	0.20	5.00	1.00	0.20	3.00
K4	0.14	3.00	5.00	1.00	6.00
K5	0.20	0.14	0.33	0.17	1.00

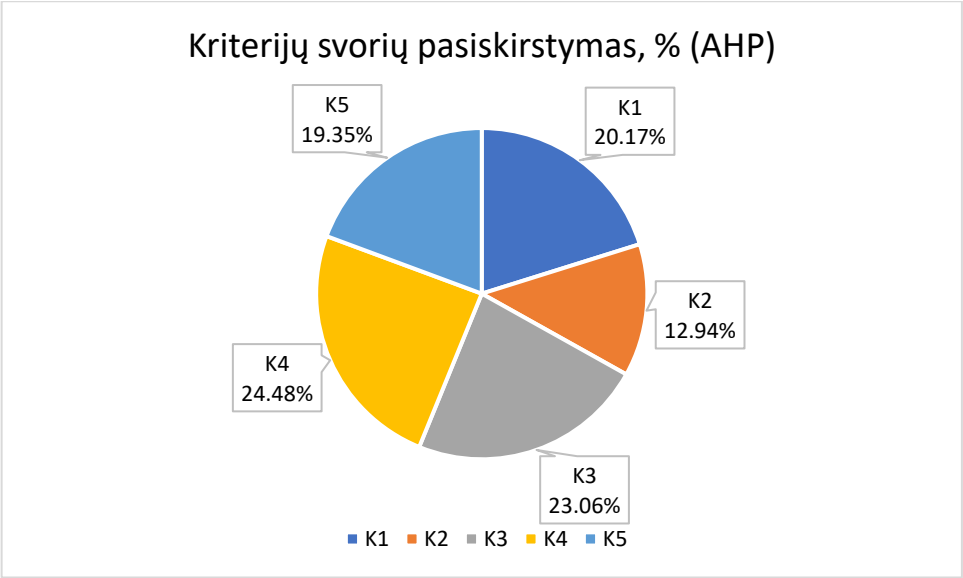
E9	K1	K2	K3	K4	K5
K1	1.00	0.33	0.20	0.14	0.25
K2	3.00	1.00	0.33	0.20	0.33
K3	5.00	3.00	1.00	0.17	0.25
K4	7.00	5.00	6.00	1.00	3.00
K5	4.00	3.00	4.00	0.33	1.00

6 pav. Ekspertinio vertinimo metu nustatyti kriterijų tarpusavio įvertinimai (AHP)

kur, E – eksperto numeris, K1 – vartotojų identifikacijos ir autentifikacijos aktualumas, K2 – prieigos kontrolės politikos nuoseklumas, K3 – atkūrimo po saugumo sutrikimų išbaigtumas, K4 – duomenų konfidencialumo užtikrinimo aiškumas, K5 – atitikties teisinei ir reguliacinei sistemai išsamumas

Eksperimentinio vertinimo metu buvo atliktas kriterijų svorių nustatymas AHP metodu pasitelkus 9 ekspertų nuomones. Kadangi ekspertų nuomonės kriterijų svorių bei svarbos nustatymo procese išsiskyrė, yra patartina apskaičiuoti jų tarpusavio suderinamumo koeficientą, siekiant įvertinti vykdymo metu gautų rezultatų patikimumą. Suderinamumo koeficientas (angl. *Consistency Ratio, CR*) gali būti apskaičiuojamas tiek rankiniu, tiek automatizuotu būdu. Šiuo atveju, pasirenkamas paprastesnis, automatizuotas sprendimas – programinė įranga *SpiceLogic AHP Process.* Nustatytas bendras ekspertinių vertinimų suderinamumo koeficientas yra vos 1,9%, šis rodiklis gali būti laikomas labai geru. Pažymėtina, kad kriterijų svorių ir svarbos nustatymo metu naudojant AHP metodą, suderinamumo koeficiento reikšmė negali viršyti numatytos 10% tolerancijos ribos, kitaip tariant, kuo labiau apskaičiuota koeficiento reikšmė yra artimesnė 0, tuo labiau ekspertų tarpusavio rezultatai yra laikomi suderintais.

Apjungus iš ekspertų gautus atskirus rezultatus, gaunami apibendrinti vertinimo duomenys. Šie duomenys yra perteikiami grafiškai (žr. 7 pav.).



7 pav. Kriterijų svorių pasiskirstymas (AHP)

kur, E – eksperto numeris, K1 – vartotojų identifikacijos ir autentifikacijos aktualumas, K2 – prieigos kontrolės politikos nuoseklumas, K3 – atkūrimo po saugumo sutrikimų išbaigtumas, K4 – duomenų konfidencialumo užtikrinimo aiškumas, K5 – atitikties teisinei ir reguliacinei sistemai išsamumas

Iš pateiktų rezultatų galima teigti, kad ekspertai, kai kalbama apie kriterijus, leidžiančius vertinti registrų ir informacinių sistemų specifikacijose apibrėžtus saugumo reikalavimus per kokybės prizmę, bene labiausiai išskyrė duomenų konfidencialumo užtikrinimo aiškumo pranašumus, – 24,48%. Toliau atitinkamai sekė atkūrimo po saugumo sutrikimų išbaigtumas (23,06%), vartotojų identifikacijos ir autentifikacijos aktualumas (20,17%) ir kiti.

Po skaitinių svorių kriterijams priskyrimo AHP metodo metu, ekspertams pateikiama sekanti apklausa (žr. 3 priedas). Joje vėl nustatomi kriterijų svoriai, tik šįkart ne skaitine, o lingvistine išraiška. Detalesnis naudojamo metodo aprašymas yra pateikiamas 2.7. poskyryje. Apibendrinti rezultatai iš ekspertinio vertinimo, kuriame nustatyti kriterijų svoriai lingvistine išraiška, pateikiami toliau (žr. 15 lentelė).

15 lentelė. Ekspertinio vertinimo metu priskirtų lingvistinių reikšmių kriterijams suvestinė

kur, E – eksperto numeris, K1 – vartotojų identifikacijos ir autentifikacijos aktualumas, K2 – prieigos kontrolės politikos nuoseklumas, K3 – atkūrimo po saugumo sutrikimų išbaigtumas, K4 – duomenų konfidencialumo užtikrinimo aiškumas, K5 – atitikties teisinei ir reguliacinei sistemai išsamumas, LA – labai aukštas, A – aukštas, V – vidutinis, Ž – žemas, LŽ – labai žemas

Kriterijus (K)	***Ekspertai (E)***								
	E1	***E2***	***E3***	***E4***	***E5***	***E6***	***E7***	***E8***	***E9***
	Eksperto priskirta lingvistinė reikšmė kriterijui K								
K1	A	LA	LA	LA	LA	LA	LA	A	V
K2	V	A	A	LA	A	A	A	A	A
K3	LA	V	LA	A	A	A	A	V	LA

Kriterijus (K)	*Ekspertai (E)*								
	E1	***E2***	***E3***	***E4***	***E5***	***E6***	***E7***	***E8***	***E9***
	Eksperto priskirta lingvistinė reikšmė kriterijui K								
K4	LA	LA	LA	V	LA	LA	LA	LA	LA
K5	A	A	A	LA	V	V	V	A	A

Siekiant lingvistine išraiška gautus rezultatus panaudoti tolimesniuose šio darbo skaičiavimuose, jie yra paverčiami (konvertuojami) į skaitines reikšmes. Konvertavimas vykdomas vadovaujantis 12 lentelėje pateikiama metodika. Toliau pateikiami po konvertavimo gauti rezultatai (žr. 16 lentelė).

16 lentelė. Ekspertų priskirtų lingvistinių reikšmių konvertavimas į skaitines

Kriterijus (K)	*Ekspertai (E)*								
	E1	***E2***	***E3***	***E4***	***E5***	***E6***	***E7***	***E8***	***E9***
	Eksperto priskirta konvertuota lingvistinė reikšmė								
K1	(0.5,0.7,0.9)	(0.7,0.9,0.9)	(0.7,0.9,0.9)	(0.7,0.9,0.9)	(0.7,0.9,0.9)	(0.7,0.9,0.9)	(0.7,0.9,0.9)	(0.5,0.7,0.9)	(0.3,0.5,0.7)
K2	(0.3,0.5,0.7)	(0.5,0.7,0.9)	(0.5,0.7,0.9)	(0.7,0.9,0.9)	(0.5,0.7,0.9)	(0.5,0.7,0.9)	(0.5,0.7,0.9)	(0.5,0.7,0.9)	(0.5,0.7,0.9)
K3	(0.7,0.9,0.9)	(0.3,0.5,0.7)	(0.7,0.9,0.9)	(0.5,0.7,0.9)	(0.5,0.7,0.9)	(0.5,0.7,0.9)	(0.5,0.7,0.9)	(0.3,0.5,0.7)	(0.7,0.9,0.9)
K4	(0.7,0.9,0.9)	(0.7,0.9,0.9)	(0.7,0.9,0.9)	(0.3,0.5,0.7)	(0.7,0.9,0.9)	(0.7,0.9,0.9)	(0.7,0.9,0.9)	(0.7,0.9,0.9)	(0.7,0.9,0.9)
K5	(0.5,0.7,0.9)	(0.5,0.7,0.9)	(0.5,0.7,0.9)	(0.7,0.9,0.9)	(0.3,0.5,0.7)	(0.3,0.5,0.7)	(0.3,0.5,0.7)	(0.5,0.7,0.9)	(0.5,0.7,0.9)

Apibendrinti konvertavimo rezultatai yra pateikiami Fuzzy TOPSIS reikšmių pavidalu (žr. 17 lentelė). Šios reikšmės gautos po ekspertų pateiktų verčių agregavimo, naudojant *Excel* skaičiavimų ruošinį.

17 lentelė. Agreguoti ekspertų rezultatai (Fuzzy)

Kriterijus (K)	*Apibendrinta reikšmė (Fuzzy)*
K1	(0.333, 0.901, 1)
K2	(0.333, 0.778, 1)
K3	(0.333, 0.802, 1)
K4	(0.333, 0.951, 1)
K5	(0.333, 0.728, 1)

Ekspertų vertinimo metu gauti rezultatai bus toliau naudojami šio darbo kontekste.

3.2.3.Specifikacijų saugumo reikalavimų vertinimas

Taikant daugiakriterius sprendimų priėmimo metodus (MCDM), labai svarbu iš anksto nustatyti pasirinkimo galimybes (alternatyvas). Kiekvieną alternatyvą būtina įvertinti ir palyginti pagal konkrečius, anksčiau ekspertų išskirtus kriterijus, kad būtų nustatoma mažiausią ir didžiausią svarbą turinti alternatyva. Alternatyvos turėtų kaip įmanoma labiau atspindėti realioje praktikoje taikomus pavyzdžius ir atspindėti įvairius potencialius sprendimo būdus, visa tai daroma su tikslu, kad analizė išliktų aktuali, reikšminga ir objektyvi.

Šiame darbe siekiama koncentruotis į registrų ir informacinių sistemų specifikacijų saugumo reikalavimų kokybės vertinimą, todėl pasirinkimo galimybėmis (alternatyvomis) nuspręsta naudoti kelių skirtingų techninių aprašų (specifikacijų) normalizuotus saugumo reikalavimų rinkinius. Kitaip tariant, ekspertui bus pateikiama tik esminė ir tiesiogiai su darbo tikslu susijusi informacija. Sudarytus rinkinius (toliau vadinamais scenarijais) ekspertai turės įvertinti per anksčiau apibrėžtų penkių kriterijų prizmę, nustatant kiekvieno iš jų svarbą tam tikram reikalavimui. Būtina paminėti, kad sudaryti rinkiniai (scenarijai) gali būti šiek tiek modifikuojami, siekiant labiau adaptuotis prie užduoties bei geriau atliepti baigiamojo darbo poreikius.

Toliau pristatomi pasirinkimo galimybių (alternatyvų) rinkiniai, kurie sudaryti iš registrų ir informacinių sistemų specifikacijų saugumo reikalavimų.

1. Scenarijus. Kraujo donorų registro (KDR) normalizuotas techninis aprašas

- *KDR naudotojai turi būti atpažįstami, o jų atliekami veiksmai žymimi naudotojų veiksmų žurnale. Programiniai moduliai turi būti prieinami naudotojams pagal jiems suteiktas teises; funkcionuoti reikalingų paslaugų teikėjo prieiga prie KDR techninės ir programinės įrangos turi būti kontroliuojama naudojant prisijungimo vardų, slaptažodžių ir teisių sistemą, skirtą darbuotojų tapatybei nustatyti;*
- *KDR naudotojai negali turėti galimybės atlikti operacijų tiesiai duomenų bazėje; duomenų bazės lygyje priėjimas prie duomenų turi būti ribojamas teisių ir rolių pagalba. Priėjimui prie duomenų bazių schemų sukurti fiksuoti sisteminiai naudotojai, kuriems leistas tik toks priėjimas kiek reikalauja KDR sistemos naudojimas; duomenų bazės administratorius neturės teisės prieiti prie duomenų failų (jei neturės galimybės prieiti prie operacinės sistemos);*
- *KDR turi užtikrinti korektišką avarinių saugumo situacijų, kurias sukėlė neteisingi KDR naudotojų veiksmai, neteisingas įvedamų duomenų formatas arba neleidžiamos įvedamų duomenų reikšmės, valdymą. Nurodytais atvejais, atlikus neteisingą (neleidžiamą) komandą*

arba nekorektiškai įvedus duomenis, KDR turi rodyti atitinkamus avarinius pranešimus ir po to grįžti į pradinę darbo būklę;

- *KDR operacinės sistemos lygyje turi būti kontroliuojamas priėjimas prie operacinės sistemos resursų, apsaugant sistemą nuo neteisėto priėjimo prie duomenų bazės failų. Operacinės sistemos lygio saugumas užtikrinamas operacinės sistemos saugumo priemonėmis;*
- *KDR įgyvendintos saugumo priemonės užtikrina apsaugą nuo OWASP (angl. „Open Web Application Security Project“) TOP 10 sąraše įvardintų saugumo pažeidimų;*

2. Scenarijus. Mokinių registro (MR) normalizuotas techninis aprašas

- *MR turi būti įgyvendinta galimybė identifikuoti prieigos prie MR duomenų autorius, fiksuoti jų atliktus veiksmus ir juos kaupti; duomenų tvarkytojams prieigos prie duomenų galimybė turi būti tik per registravimosi ir slaptažodžių sistemą;*
- *Prieigos prie MR elektroninės informacijos teises gali suteikti tik MR administratorius. Registro naudotojams suteikiamos tik jų funkcijoms vykdyti būtinos teisės; Visos užklausos į duomenų bazes yra fiksuojamos programiniu būdu, pilnai identifikuojant užklausos autorių ir atliekamą veiksmą;*
- *DBVS turi būti naudojamas LOG failas, kad reikiamu atveju (įvykus avarinei situacijai) pats duomenų bazių serveris atstatytų duomenų bazę iki korektiškos būsenos;*
- *MR naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo; viešaisiais telekomunikaciniais tinklais perduodamos elektroninės informacijos konfidencialumas užtikrinamas naudojant HTTPS (Hypertext Transfer Protocol Secure) protokolą arba šifravimą; užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą iš kitų valstybės institucijų, naudojami saugūs ryšio kanalai, kuriais perduodami šifruoti duomenys;*
- *Būtina sąlyga duomenų apsaugai realizuoti yra norminių aktų, reglamentuojančių duomenų teisinę apsaugą, įgyvendinimas: Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas; Mokinių registro duomenų saugos nuostatai; Bendrųjų elektroninės informacijos saugos reikalavimų aprašas“;*
- *Sistema turi būti sukurta vadovaujantis Lietuvos standartais LST ISO/IEC 27001:2013, LST ISO/IEC 27002:2014 ir kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais; Sąsaja naudotojui turi atitikti W3C standartus ir rekomendacijas;*

3. Scenarijus. Valstybės informacinių technologijų paslaugų valdymo informacinės sistemos (VIPVIS) normalizuotas techninis aprašas

- *Kiekvienas darbuotojas turi asmeninę magnetinę kortelę ir įeidamas į pastatą arba išeidamas iš jo pasižymi įėjimo punktuose; lankytojams ir svečiams privalomai išduodamos svečio elektroninės kortelės. Už apsilankymą atsakingas darbuotojas pasirašo įėjimo punkto žurnale už kiekvieną lankytoją; po 18 val. vakaro ir nedarbo dienomis į pastatą patekti gali tiktai specialius leidimus turintys darbuotojai;*
- *Prisijungti prie kompiuterinio tinklo naudojami VIPVIS naudotojų ID ir prieigos teisių sistema, pagal kurią nustatomos naudotojų teisės tinkle; nuotolinis prisijungimas prie VIPVIS vykdomas protokolu, skirtu duomenims šifruoti; pagal VIPVIS naudotojų atliekamas funkcijas jiems turi būti priskiriami atitinkami prieigos teisių rinkiniai;*
- *VIPVIS administratoriaus naudojamame kompiuteryje turi būti nustatytas VIPVIS naudotojo prieigos blokavimas po tam tikro neaktyvumo laikotarpio, būtina naudoti ekrano apsaugos programą (angl. Screensaver). Neaktyvumo laikotarpis negali būti ilgesnis kaip 15 minučių; saugant vietinį tinklą arba nenaudojamas tinklo jungtis, ribojama fizinė prieiga prie tinklo kabelių, skirstytuvų, atšakų, kartotuvų ir antgalių;*
- *Dingus elektros įtampai sistema automatiškai informuoja atsakingus darbuotojus apie (saugumo) gedimą; esant elektros srovės tiekimo sutrikimų, serverių įrangos veikimas garantuojamas ne mažiau nei 30 minučių ir užtikrinamas saugus programų uždarymas kompiuteriuose, jeigu elektros tiekimas neatsinaujintų;*
- *VIPVIS administratoriaus naudojama kompiuterinė įranga ir elektroninės informacijos laikmenos turi būti laikomos taip, kad pašaliniai asmenys negalėtų prie jų prieiti, paimti ar sugadinti; VIPVIS naudojamos saugumo priemonės užtikrina apsaugą nuo OWASP (angl. „Open Web Application Security Project“) TOP 10 sąraše įvardintų saugumo pažeidimų;*

4. Scenarijus. Žvejybos sektoriaus perleidžiamųjų teisių registro (PTR) normalizuotas techninis aprašas

- *Kiekvienas PTR naudotojas turi būti unikaliai identifikuojamas. Visa identifikavimo informacija turi būti saugoma šifruotu pavidalu tokiu būdu, kad iš saugomos informacijos būtų neįmanoma atkurti pirminių duomenų (pavyzdžiui, slaptažodžių); PTR naudotojas turi patvirtinti savo tapatybę slaptažodžiu arba kitomis nustatytomis identifikavimo ir autentifikavimo patvirtinimo priemonėmis;*
- *PTR turi užtikrinti galimybę nustatyti skirtingus teisių sąrašus pagal PTR naudotojo prisijungimo tipą ir jo tapatybės patikrinimo metodo patikimumą; PTR turi būti prieinamas naudojantis bendromis PTR teikiamomis saugos priemonėmis, bendro prisijungimo (angl.*

Single Sign On – SSO) principu; Turi būti patvirtinti asmenų, kuriems suteiktos PTR administratoriaus teisės prisijungti prie PTR, sąrašai ir periodiškai peržiūrimi informacijos saugos specialisto. Sąrašas turi būti nedelsiant peržiūrėtas, kai įstatymų nustatytais atvejais PTR administratorius nušalinamas nuo darbo pareigų;

- *Užtikrinant PTR atkūrimą gedimo atveju turi būti daromos reguliarios rezervinės programos ir duomenų bazės kopijos. Įvykus (saugumo) gedimui, PTR atkūrimo laikas (angl. Recovery Time) turi būti ne ilgesnis kaip 1 darbo diena;*
- *PTR turi palaikyti siunčiamų, gaunamų ir saugomų duomenų užšifravimą ir iššifravimą; Audito duomenys turi būti archyvuojami. Archyve saugomi duomenys turi būti apsaugoti nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo;*
- *Turi būti įgyvendintos LST ISO/IEC 27001:2013 nurodytos techninės saugos priemonės, išskyrus priemones, kurios netaikytinos dėl PTR tvarkytojo veiklos ar PTR naudojamos techninės įrangos pobūdžio. PTR kuriamas vadovaujantis Lietuvos standartais LST ISO/IEC 27001:2013, LST ISO/IEC 27002:2014 ir kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais;*

5. Scenarijus. Nacionalinės turizmo informacinės sistemos (NTIS) normalizuotas techninis aprašas

- *NTIS naudotojui prisijungus prie NTIS naudojant vardų, slaptažodžių ir teisių sistemą, turi būti pateikiama sukonfigūruota naudotojo darbo aplinka ir tik jam prieinami darbui būtini duomenys;*
- *NTIS turi būti atliekamos reguliarios rezervinės programų ir duomenų bazių kopijos; NTIS turi leisti atkurti duomenis iš rezervinių duomenų kopijų;*
- *NTIS turi visapusiškai užtikrinti duomenų konfidencialumą taikydama šifravimą perduodamiems duomenims; pašalinių asmenų priėjimas prie kompiuterinės įrangos ir laikmenų turi būti užkardytas;*
- *NTIS saugumo priemonės turi užtikrinti apsaugą nuo OWASP (angl. Open Web Application Security Project) TOP 10 sąraše įvardintų saugumo pažeidimų;*

Pristatyti registrų ir informacinių sistemų specifikacijų saugumo reikalavimų rinkiniai (scenarijai) bus vertinami vadovaujantis sudaryta vertinimo metodika, ji bei kita aktuali informacija yra pateikiama ekspertinės apklausos formoje (žr. 4 priedas).

Naujojo (siūlomo) daugiakriterio saugumo reikalavimų kokybės vertinimo metodo taikymas buvo atliktas 4 ekspertų. Paminėtina, kad kokybės vertinimo metodą naudoję ekspertai yra iš pradinės 9 ekspertų grupės. 4 ekspertai įvertino 5 skirtingus registrų ir

informacinių sistemų specifikacijų saugumo reikalavimų rinkinius (scenarijus), vadovaudamiesi ankstesnių apklausų metu identifikuotais vertinimo kriterijais. Ekspertinio vertinimo metu gauti rezultatai, kurie bus naudojami WASPAS skaičiavimuose, pristatomi 6 priede (žr. 6 priedas). Kaip pristato ekspertų vertinimo suvestinės, ekspertų nuomonės, įvertinant saugumo reikalavimų rinkinių kokybę, nebuvo vienareikšmės ir išsiskyrė tarpusavyje.

Kadangi saugumo reikalavimų rinkinių kokybės reitingo nustatymas bus vykdomas skaičiuojant tiek WASPAS, tiek Fuzzy TOPSIS metodais, 7 priede pateikiamos lingvistinės (kokybinės) reikšmės, kurios buvo konvertuotos iš 6 priede pateiktų vertinimo suvestinių skaitinių (kiekybinių) reikšmių (žr. 6 priedas) (žr. 7 priedas).

Pažymėtina, kad ekspertinio vertinimo metu buvo pasirinkta 1–5 balų vertinimo skalė, kadangi ji yra lengvai suprantama, neapkrauna vertintojų ir leidžia greitai bei efektyviai pateikti jų nuomonę atspindintį sprendimą (skaitinę reikšmę). Platesnės vertinimo skalės (pvz., 1–10) naudojimas reikalauja didesnio ekspertų dėmesio ir laiko, o tai galėtų sumažinti vertinimo nuoseklumą, ištęsti užduoties atlikimo laiką.

Konvertuotos reikšmės bus taikomos tolesniame darbe, atliekant Fuzzy TOPSIS skaičiavimus.

3.2.4.Specifikacijų saugumo reikalavimų rinkinių kokybės reitingo nustatymas

Šioje dalyje, naudojant ekspertų nuomones, siekiama sudaryti registrų ir informacinių sistemų specifikacijų saugumo reikalavimų rinkinių (scenarijų) kokybės reitingą. Šis reitingas atspindės kiekvienos iš vertinamų alternatyvų saugumo reikalavimų apibrėžties kokybės lygį. Kitaip tariant, bus nustatyta, kuris scenarijus, ekspertų nuomone, yra vertinamas kaip tinkamiausią kokybės lygį pristatantis dokumentas, o kuris - privalo būti koreguotinas.

Specifikacijų saugumo reikalavimų rinkinių (scenarijų) kokybės reitingo nustatymas pradedamas nuo skaičiavimų WASPAS metodu atlikimo – detalesnė metodo pritaikymo informacija bei taikytos formulės yra pateikiamos 2.6. poskyryje.

1. Remiantis ekspertų priskirtais įverčiais, suformuojama sprendimo priėmimo matrica. Ji užpildoma įverčių vidurkiais (5 formulė)

18 lentelė. Įverčių vidurkiais užpildyta sprendimo priėmimo matrica (WASPAS metodas)

Kriterijus / *Scenarijus*	***K1***	***K2***	***K3***	***K4***	***K5***
1	3.75	4.25	3.25	3.75	2.75
2	3.25	3.75	3.5	3.25	3.75

Kriterijus / *Scenarijus*	*K1*	*K2*	*K3*	*K4*	*K5*
3	4.25	4.25	4	4	4
4	4	3.5	4	4.25	4.5
5	2.75	2.75	2.75	2.5	2.5

2. Sekantis veiksmas – įverčių vidurkių matricos normalizavimas. Taikoma normalizacijos naudingam kriterijui formulė (6 formulė)

19 lentelė. Normalizuota įverčių vidurkių sprendimo priėmimo matrica (WASPAS metodas)

Kriterijus / *Scenarijus*	*K1*	*K2*	*K3*	*K4*	*K5*
1	0.88	1	0.81	0.88	0.61
2	0.76	0.88	0.88	0.76	0.83
3	1	1	1	0.94	0.89
4	0.94	0.82	1	1	1
5	0.65	0.65	0.69	0.59	0.56

3. Toliau apskaičiuojamas pirmasis optimalumo kriterijus (Q1) remiantis 8 formule (WSM)

20 lentelė. Scenarijams apskaičiuotos pirmojo optimalumo kriterijaus (Q1) vertės (WASPAS metodas)

Scenarijaus Nr.	*Q1*
1 (KDR)	0.829
2 (MR)	0.819
3 (VIPVIS)	0.964
4 (PTR)	0.965
5 (NTIS)	0.624

4. Taip pat apskaičiuojamas ir antrasis optimalumo kriterijus (Q2) remiantis 9 formule (WPM)

21 lentelė. Scenarijams apskaičiuotos antrojo optimalumo kriterijaus (Q2) vertės (WASPAS metodas)

Scenarijaus Nr.	*Q2*
1 (KDR)	0.819

Scenarijaus Nr.	*Q2*
2 (MR)	0.817
3 (VIPVIS)	0.963
4 (PTR)	0.963
5 (NTIS)	0.622

5. Optimalumo kriterijų apibendrintas agregavimas, kai naudojamos dvi – 10 ir 11 formulės. Gaunamas pagrindinis sprendimo priėmimo kriterijus *Q*

22 lentelė. Sprendimo priėmimo kriterijaus Q vertės apskaičiavimas (WASPAS metodas)

Scenarijaus Nr.	*Q1*	*Q2*	*Q*
1 (KDR)	0.829	0.819	0.824
2 (MR)	0.819	0.817	0.818
3 (VIPVIS)	0.964	0.963	0.963
4 (PTR)	0.965	0.963	0.964
5 (NTIS)	0.624	0.622	0.623

6. Remiantis skaičiavimų rezultatais, nustatomas saugumo reikalavimų rinkinių (scenarijų) reitingas

23 lentelė. Scenarijų kokybės reitingo nustatymo rezultatai (WASPAS metodas)

Scenarijaus Nr.	*Q*	*Reitingas*
1 (KDR)	0.824	3
2 (MR)	0.818	4
3 (VIPVIS)	0.963	2
4 (PTR)	0.964	1
5 (NTIS)	0.623	5

Atlikus scenarijų kokybės reitingo skaičiavimus WASPAS metodu, galima teigti, kad tarp pateiktų alternatyvų, ekspertų nuomone, geriausią saugumo reikalavimų apibrėžtį kokybei atitiko PTR normalizuotas techninis aprašas (Q - 0.964), todėl PTR specifikacijoje apibrėžti saugumo reikalavimai yra vertinami kaip labiausiai tinkamą kokybės lygį pristatantys saugumo reikalavimai (žr. 5 lentelė). Antra geriausia alternatyva išreitinguotas VIPVIS scenarijus (Q - 0.963), kuris nuo pirmos vietos atsiliko vos tūkstantųjų dalimis. Ekspertų nuomone, prasčiausią saugumo reikalavimų kokybės apibrėžtį pristatė NTIS normalizuotas techninis aprašas – ši

alternatyva, penkių pateiktų vertinimo alternatyvų kontekste, atitinka koreguotiną kokybės lygį ir privalo būti tobulinama (žr. 5 lentelė).

Toliau saugumo reikalavimų rinkinių kokybės reitingo nustatymas apskaičiuojamas taikant Fuzzy TOPSIS metodą.

1. Vėl sudaroma sprendimo priėmimo matrica, ji užpildoma trišalių įvertinimų agreguotais vidurkiais (15, 16 formulės)

24 lentelė. Trišalių įvertinimų agreguotais vidurkiais užpildyta sprendimo priėmimo matrica (Fuzzy TOPSIS metodas)

Kriterijus / *Scenarijus*	***K1***	***K2***	***K3***	***K4***	***K5***
1	(3, 6.5, 9)	(3, 7.5, 9)	(3, 5.5, 9)	(3, 6.5, 9)	(1, 4.5, 9)
2	(1, 5.5, 9)	(3, 6.5, 9)	(1, 6, 9)	(1, 5.5, 9)	(3, 6.5, 9)
3	(3, 7.5, 9)	(3, 7.5, 9)	(3, 7, 9)	(3, 7, 9)	(3, 7, 9)
4	(3, 7, 9)	(1, 6, 9)	(3, 7, 9)	(3, 7.5, 9)	(3, 8, 9)
5	(1, 4.5, 7)	(1, 4.5, 7)	(1, 4.5, 7)	(1, 4, 7)	(1, 4, 7)

2. Atliekama matricos agreguotų vidurkių normalizacija (17 formulė)

25 lentelė. Normalizuota agreguotų įverčių vidurkių sprendimo priėmimo matrica (Fuzzy TOPSIS metodas)

Kriterijus / *Scenarijus*	***K1***	***K2***	***K3***	***K4***	***K5***
1	(0.33, 0.72, 1.00)	(0.33, 0.83, 1.00)	(0.33, 0.61, 1.00)	(0.33, 0.72, 1.00)	(0.11, 0.50, 1.00)
2	(0.11, 0.61, 1.00)	(0.33, 0.72, 1.00)	(0.11, 0.67, 1.00)	(0.11, 0.61, 1.00)	(0.33, 0.72, 1.00)
3	(0.33, 0.83, 1.00)	(0.33, 0.83, 1.00)	(0.33, 0.78, 1.00)	(0.33, 0.78, 1.00)	(0.33, 0.78, 1.00)
4	(0.33, 0.78, 1.00)	(0.11, 0.67, 1.00)	(0.33, 0.78, 1.00)	(0.33, 0.83, 1.00)	(0.33, 0.89, 1.00)
5	(0.11, 0.50, 0.78)	(0.11, 0.50, 0.78)	(0.11, 0.50, 0.78)	(0.11, 0.44, 0.78)	(0.11, 0.44, 0.78)

3. Vykdoma agreguotų vidurkių matricos svertinė normalizacija (naudojami Fuzzy TOPSIS svoriai kriterijams (žr. 4.4. lentelė))

26 lentelė. Agreguotų vidurkių svertinė normalizuota matrica (Fuzzy TOPSIS metodas)

Kriterijus / *Scenarijus*	***K1***	***K2***	***K3***	***K4***	***K5***
1	(0.11, 0.65, 1.00)	(0.11, 0.65, 1.00)	(0.11, 0.49, 1.00)	(0.11, 0.69, 1.00)	(0.04, 0.36, 1.00)
2	(0.04, 0.55, 1.00)	(0.11, 0.56, 1.00)	(0.04, 0.53, 1.00)	(0.04, 0.58, 1.00)	(0.11, 0.53, 1.00)

Kriterijus / Scenarijus	K1	K2	K3	K4	K5
3	(0.11, 0.75, 1.00)	(0.11, 0.65, 1.00)	(0.11, 0.62, 1.00)	(0.11, 0.74, 1.00)	(0.11, 0.57, 1.00)
4	(0.11, 0.70, 1.00)	(0.04, 0.52, 1.00)	(0.11, 0.62, 1.00)	(0.11, 0.79, 1.00)	(0.11, 0.65, 1.00)
5	(0.04, 0.45, 0.78)	(0.04, 0.39, 0.78)	(0.04, 0.40, 0.78)	(0.04, 0.42, 0.78)	(0.04, 0.32, 0.78)

4. Nustatoma labiausiai teigiamai ideali vertė A^* bei labiausiai neigiamai ideali vertė A^- (18, 19 formulės)

27 lentelė. Teigiamai ir neigiamai idealios vertės (Fuzzy TOPSIS metodas)

Kriterijus	A* (teigiamai ideali)	A^- (neigiamai blogiausia)
K1	(0.11, 0.75, 1.00)	(0.04, 0.45, 0.78)
K2	(0.11, 0.65, 1.00)	(0.04, 0.39, 0.78)
K3	(0.11, 0.62, 1.00)	(0.04, 0.40, 0.78)
K4	(0.11, 0.79, 1.00)	(0.04, 0.42, 0.78)
K5	(0.11, 0.65, 1.00)	(0.04, 0.32, 0.78)

5. Apskaičiuojami toliai (atstumai) d_i^* ir d_i^- tarp alternatyvų (atstumas tarp teigiamai A^* ir neigiamai A^- idealaus sprendimo) (20, 21 formulės)

28 lentelė. Tolis tarp teigiamai idealių verčių ir alternatyvų-scenarijų (Fuzzy TOPSIS metodas)

Kriterijus / Scenarijus	K1	K2	K3	K4	K5
1	0.06	0.00	0.08	0.06	0.17
2	0.12	0.05	0.07	0.13	0.07
3	0.00	0.00	0.00	0.03	0.05
4	0.03	0.09	0.00	0.00	0.00
5	0.22	0.20	0.19	0.25	0.23

29 lentelė. Tolis tarp neigiamai idealių verčių ir alternatyvų-scenarijų (Fuzzy TOPSIS metodas)

Kriterijus / Scenarijus	K1	K2	K3	K4	K5
1	0.18	0.20	0.14	0.20	0.13
2	0.14	0.17	0.15	0.16	0.18
3	0.22	0.20	0.19	0.23	0.19

Kriterijus / *Scenarijus*	*K1*	*K2*	*K3*	*K4*	*K5*
4	0.20	0.15	0.19	0.25	0.23
5	0.00	0.00	0.00	0.00	0.00

Kartu yra apskaičiuojamos galutinės atstumo reikšmės visoms alternatyvoms-scenarijams (pavienių reikšmių agregavimas)

30 lentelė. Galutinės (agreguotos) atstumų vertės alternatyvoms (Fuzzy TOPSIS metodas)

Scenarijus	*di**	*di-*
1	0.36	0.86
2	0.44	0.79
3	0.08	1.03
4	0.12	1.02
5	1.09	0.00

6. Galiausiai, atliekami skaičiavimai kiekvienos iš alternatyvų artumo koeficientui rasti (22 formulė)

31 lentelė. Alternatyvų artumo koeficientų vertės (Fuzzy TOPSIS metodas)

Scenarijaus Nr.	C_i	*Reitingas*
1 (KDR)	0.70	3
2 (MR)	0.64	4
3 (VIPVIS)	0.93	1
4 (PTR)	0.90	2
5 (NTIS)	0.00	5

Atlikus scenarijų kokybės reitingo skaičiavimus Fuzzy TOPSIS metodu, galima teigti, kad tarp pateiktų alternatyvų, ekspertų nuomone, geriausią saugumo reikalavimų apibrėžtį kokybei atitiko VIPVIS normalizuotas techninis aprašas (Ci - 0.93), todėl VIPVIS specifikacijoje apibrėžti saugumo reikalavimai yra vertinami kaip labiausiai tinkamą kokybės lygį pristatantys saugumo reikalavimai (žr. 5 lentelė). Antra geriausia alternatyva išreitinguotas PTR scenarijus (C_i - 0.90). Ekspertų nuomone, prasčiausią (koreguotiną lygį) saugumo reikalavimų kokybės apibrėžtį pristatė NTIS normalizuotas techninis aprašas.

Pažymėtina, kad alternatyvai NTIS artumo koeficientas *Ci* yra lygus nuliui dėl labai didelio ekspertinio vertinimo sutapimo su neigiamai idealiu sprendimu (A^-). Tokiais atvejais,

kai ekspertai vieningai vertina alternatyvą kaip žemiausią pagal visus kriterijus, alternatyva natūraliai atitinka blogiausią scenarijų. Šis rezultatas yra matematiškai pagrįstas ir nevertinamas kaip metodinė klaida.

Paminėtina, kad alternatyvų (scenarijų) reitingas, apskaičiuotas atitinkamai su WASPAS ir Fuzzy TOPSIS metodais, galutiniame rezultate šiek tiek išsiskyrė. Prasčiausia alternatyva, ekspertų nuomone, išliko NTIS scenarijus, tačiau geriausia alternatyva – pasikeitė. Lyderiai apsimainė vietomis, t.y. WASPAS metode pirmavęs PTR scenarijus Fuzzy TOPSIS skaičiavimuose liko antras, o VIPVIS scenarijus buvo nustatytas kaip labiausiai tinkamą (geriausią) saugumo reikalavimų kokybės lygį pristatantis scenarijus. Tai galima paaiškinti dėl skirtingų metodų vykdymo metodikų, kur išsiskiria kriterijų svorių nustatymo principai bei kitų objektyvių aplinkybių.

3.3.Ekspertų nuomonių suderinamumo apskaičiavimas

Siekiant visapusiškiau atskleisti ekspertų nuomonių suderinamumo vertinimo rodiklio jautrumą, buvo priimtas sprendimas iki šiol naudotą penkiabalę vertinimo skalę transformuoti į dešimtbalę skalę. Tokia praktika sudaro palankias sąlygas pagerinti atskirtį tarp vertintų alternatyvų, išvengti vienodų įverčių priskyrimo bei padidinti rezultatų tikslumą. Būtina pažymėti, kad tiesinė vertinimo skalės transformacija išlaiko proporcingą reikšmių struktūrą, todėl ekspertų vertinimai negali būti iškraipomi ar kitaip modifikuojami.

Esminis faktorius vertinimo skalės transformacijai yra geresnis suderinamumas su statistiniais metodais, pvz., Kendallio metodika. Tą galima nesunkiai pagrįsti, nes Kendallio suderinamumo vertinimo rodiklis *w* itin pakantus dispersijoms (verčių nuokrypiams).

Ekspertų nuomonių suderinamumo skaičiavimas išlieka itin svarbiu žingsniu, kada kalbama apie nuomones. Nereikėtų pamiršti, kad vertinimą atliekantys ekspertai nėra robotai – jie vertinimus gali atlikti remdamiesi asmeniškumais, vedini emocijų, galiausiai, jie gali būti tiesiog subjektyvūs. Todėl, siekiant įsitikinti, kad nei viena iš šių ar kitų rizikų neturėjo neigiamos įtakos ekspertinio vertinimo procesui, yra siekiama apskaičiuoti rodiklį, kuris leistų įsitikinti ekspertų nuomonių tarpusavio sutarimu – Kendallio konkordancijos koeficientą *w.* Detalesnė informacija, taikytinos formulės bei skaičiavimo etapai yra pateikiami 2.8. poskyryje.

Norint apskaičiuoti Kendallio konkordancijos koeficientą *w,* prieš tai būtina apskaičiuoti tokius rodiklius: kiekvienos alternatyvos reikšmių sumą e_i (23 formulė), reikšmių vidurkį $\bar{e}$ (24 formulė) bei nuokrypį nuo bendro vidurkio S (25 formulė). Tuomet rodikliai yra

įstatomi į pagrindinę formulę (26 formulė) ir, galiausiai, apskaičiuojamas konkordancijos koeficientas *w*:

$$w = \frac{(12 * 110.4)}{(4^2((5^3) - 5))} = \sim 0.69$$

Apskaičiuotas koeficientas *w* yra ~0.69. Šis solidus skaičius iš dalies įrodo, kad ekspertų nuomonių suderinamumas yra pakankamai aukštas.

Siekiant būti visiškai įsitikinus, kad ekspertų nuomonės gali būti laikomos suderintomis, kartu rekomenduotina apskaičiuoti ir kitą, chi-kvadrato $\mathcal{X}^2$ rodiklį, skirtą konkordancijos koeficiento reikšmingumui nustatyti (28 formulė):

$$\mathcal{X}^2 = \frac{12 * 110.4}{4 * 5(5 + 1)} = 11.04$$

Tuomet šis rodiklis turi būti lyginamas su $\mathcal{X}^2$ kritiniu rodikliu X_{kr}^2. Jeigu $\mathcal{X}^2 \geq X_{kr}^2$, tuomet laikoma, kad nuomonių suderinamumas yra statistiškai reikšmingas (taip pat pagrindžiamas *w* rodiklio patikimumas).

$$X_{kr}^2\ (v = m - 1, kai\ \alpha = 0.05) = 9.4877$$

Remiantis moksline literatūra ir apskaičiuotomis vertėmis galima daryti išvadą, kad ekspertų nuomonių suderinamumas yra išties vieningas – aukštesnė nei 0.60 (*w* - ~0.69) *w* vertė leidžia drąsiai interpretuoti, kad ekspertus vienija stiprus sutarimas (žr. 13 lentelė). Tai pagrindžia ir koeficiento reikšmingumo vertės lyginimas su jo kritine verte: $\mathcal{X}^2 \geq X_{kr}^2$ $(11.04 \geq 9.4877)$ – ekspertų nuomonės yra statistiškai reikšmingai suderintos.

3.4.Daugiakriterių metodų jautrumo analizė

Daugiakriterių sprendimų priėmimo metodų jautrumo analizė yra esminė tyrimo dalis, leidžianti įvertinti, kiek stabilūs yra galutiniai sprendimai esant tam tikrų pradinių duomenų pokyčiams. Jautrumo analizė padeda nustatyti, ar sprendimas išlieka patikimas, kai sąlygos šiek tiek keičiasi, bei leidžia identifikuoti situacijas, kuriose sprendimas tampa jautrus ar mažiau stabilus. Tokiu būdu jautrumo analizė padeda pagrįsti metodo pasirinkimą, sustiprina rezultato interpretaciją ir užtikrina didesnį pasitikėjimą priimtu sprendimu.

Pirmasis WASPAS metodo jautrumo testavimo metodas – kiekvienos iš penkių kriterijų svertinės reikšmės keitimas (didinimas, mažinimas) 5%.

Pirmojo kriterijaus (K1) svertinių reikšmių keitimo rezultatai:

32 lentelė. WASPAS metodo jautrumo testavimas koreguojant K1 svertines reikšmes – pirmasis metodas

Scenarijaus Nr.	Svertinės reikšmės K (kai K1 + 5%)	Optimalumo reikšmės Q (kai K1 + 5%)	Reitingas (kai K1 + 5%)	Svertinės reikšmės K (kai K1 - 5%)	Optimalumo reikšmės Q (kai K1 - 5%)	Reitingas (kai K1 - 5%)
1	0.2097	0.82481	3	0.1936	0.82366	3
2	0.1281	0.81731	4	0.1307	0.81840	4
3	0.2283	0.96394	2	0.2329	0.96322	2
4	0.2424	0.96409	1	0.2473	0.96456	1
5	0.1916	0.62357	5	0.1955	0.62310	5

Kaip matoma, alternatyvų reitingas nepakito.

Antrojo kriterijaus (K2) svertinių reikšmių keitimo rezultatai:

33 lentelė. WASPAS metodo jautrumo testavimas koreguojant K2 svertines reikšmes – pirmasis metodas

Scenarijaus Nr.	Svertinės reikšmės K (kai K2 + 5%)	Optimalumo reikšmės Q (kai K2 + 5%)	Reitingas (kai K2 + 5%)	Svertinės reikšmės K (kai K2 - 5%)	Optimalumo reikšmės Q (kai K2 - 5%)	Reitingas (kai K2 - 5%)
1	0.2004	0.82532	3	0.2030	0.82315	3
2	0.1350	0.81826	4	0.1237	0.81744	4
3	0.2291	0.96382	1	0.2321	0.96335	2
4	0.2432	0.96338	2	0.2464	0.96527	1
5	0.1923	0.62349	5	0.1948	0.62319	5

Pateiktoje lentelėje įžvelgiami pasikeitimai tarp alternatyvų reitinge. Dvi, geriausiai įvertintos alternatyvos, apsikeitė vietomis – 4 alternatyva užleido pirmąją vietą 3 alternatyvai.

Trečiojo kriterijaus (K3) svertinių reikšmių keitimo rezultatai:

34 lentelė. WASPAS metodo jautrumo testavimas koreguojant K3 svertines reikšmes – pirmasis metodas

Scenarijaus Nr.	Svertinės reikšmės K (kai K3 + 5%)	Optimalumo reikšmės Q (kai K3 + 5%)	Reitingas (kai K3 + 5%)	Svertinės reikšmės K (kai K3 - 5%)	Optimalumo reikšmės Q (kai K3 - 5%)	Reitingas (kai K3 - 5%)
1	0.1994	0.82411	3	0.2041	0.82438	3
2	0.1279	0.81849	4	0.1309	0.81719	4
3	0.2394	0.96399	2	0.2216	0.96316	2
4	0.2420	0.96472	1	0.2477	0.96391	1
5	0.1913	0.62405	5	0.1958	0.62261	5

Kaip matoma, alternatyvų reitingas nepakito.

Ketvirtojo kriterijaus (K4) svertinių reikšmių keitimo rezultatai:

35 lentelė. WASPAS metodo jautrumo testavimas koreguojant K4 svertines reikšmes – pirmasis metodas

Scenarijaus Nr.	Svertinės reikšmės K (kai K4 + 5%)	Optimalumo reikšmės Q (kai K4 + 5%)	Reitingas (kai K4 + 5%)	Svertinės reikšmės K (kai K4 - 5%)	Optimalumo reikšmės Q (kai K4 - 5%)	Reitingas (kai K4 - 5%)
1	0.1993	0.82493	3	0.2042	0.82354	3
2	0.1278	0.81720	4	0.1310	0.81852	4
3	0.2278	0.96331	2	0.2335	0.96386	2
4	0.2539	0.96475	1	0.2354	0.96388	1
5	0.1912	0.62291	5	0.1959	0.62378	5

Kaip matoma, alternatyvų reitingas nepakito.

Penktojo kriterijaus (K5) svertinių reikšmių keitimo rezultatai:

36 lentelė. WASPAS metodo jautrumo testavimas koreguojant K5 svertines reikšmes – pirmasis metodas

Scenarijaus Nr.	Svertinės reikšmės K (kai K5 + 5%)	Optimalumo reikšmės Q (kai K5 + 5%)	Reitingas (kai K5 + 5%)	Svertinės reikšmės K (kai K5 - 5%)	Optimalumo reikšmės Q (kai K5 - 5%)	Reitingas (kai K5 - 5%)
1	0.1998	0.82354	3	0.2037	0.82648	3
2	0.1282	0.81852	4	0.1307	0.81770	4

Scenarijaus Nr.	Svertinės reikšmės K (kai K5 + 5%)	Optimalumo reikšmės Q (kai K5 + 5%)	Reitingas (kai K5 + 5%)	Svertinės reikšmės K (kai K5 - 5%)	Optimalumo reikšmės Q (kai K5 - 5%)	Reitingas (kai K5 - 5%)
3	0.2284	0.96386	2	0.2329	0.96433	1
4	0.2425	0.96388	1	0.2472	0.96397	2
5	0.2012	0.62378	5	0.1856	0.62402	5

Pateiktoje lentelėje įžvelgiami pasikeitimai tarp alternatyvų reitinge. Dvi, geriausiai įvertintos alternatyvos, apsikeitė vietomis – 4 alternatyva užleido pirmąją vietą 3 alternatyvai.

Atliekant WASPAS metodo jautrumo analizės skaičiavimus vadovaujantis pirmuoju metodu (koreguojant pavienių kriterijų svertines reikšmes ±5%) buvo nustatyta, kad esant tokiems pokyčiams, dvi aukščiausiai įvertinamos alternatyvos tam tikrais atvejais apsikeičia vietomis reitingo lentelėje. Visgi šių alternatyvų galutinės sprendimo priėmimo Q reikšmės skyrėsi mažiau nei tūkstantosiomis skaičiaus dalimis, todėl toks pozicijų pasikeitimas laikytinas nežymiu ir neturinčiu esminės įtakos sprendimo priėmimui.

Antrasis metodas WASPAS metodo jautrumui testuoti yra visų kriterijų svertinių verčių sulyginimas (visi kriterijų svoriai tampa lygūs) (žr. 37 lentelė).

37 lentelė. WASPAS metodo jautrumo testavimas sulyginant kriterijų svertines reikšmes – antrasis metodas

Scenarijaus Nr.	Svertinės reikšmės K	Optimalumo reikšmės Q	Reitingas
1	0.20	0.83	3
2	0.20	0.82	4
3	0.20	0.96	1
4	0.20	0.95	2
5	0.20	0.62	5

Atlikus WASPAS metodo jautrumo analizę antruoju testavimo metodu (sulyginant skirtingas kriterijų svertines reikšmes), nustatyta, kad metodo jautrumo rezultatai tam tikrais atvejais gali būti jautresni. Skaičiavimai pristatė, kad esant labai artimoms kriterijų svorių reikšmėms bei apylygiam ekspertų vertinimui, reitingo lentelėje gali įvykti reikšmingesni pasikeitimai – geriausiai įvertintos alternatyvos apsikeitė vietomis, o jų Q reikšmių skirtumas siekė šimtąsias skaičiaus dalis. Tokie rezultatai leidžia teigti, kad nors WASPAS metodas iš

esmės yra stabilus, jis gali būti jautresnis esant mažiems skirtumams tarp kriterijų svorių ir ekspertų vertinimų, todėl tokiose situacijose rekomenduojama sprendimus papildomai pagrįsti, įsivesti saugiklius arba laikyti keletą geriausių alternatyvų lygiavertėmis.

Taikytų metodų jautrumo analizė yra tęsiama su Fuzzy TOPSIS metodu. Fuzzy TOPSIS metodo jautrumo testavimas – *fuzzy* trišalės (*l, m, u*) skaitinės svertinės vertės *m* keitimas (didinimas ir mažinimas) kiekvienam kriterijui 10%.

Pirmojo kriterijaus (K1) svertinės vidurinės *m* vertės keitimo rezultatai:

38 lentelė. Fuzzy TOPSIS metodo jautrumo testavimas koreguojant K1 svertinę reikšmę m

Scenarijaus Nr.	Fuzzy trišalės normalizuotos svertinės vertės *m* svoris (kai K1 *m* vertė + 10%)	Alternatyvų artumas, Ci (kai K1 *m* vertė + 10%)	Reitingas (kai K1 *m* vertė + 10%)	Fuzzy trišalės normalizuotos svertinės vertės *m* svoris (kai K1 *m* vertė - 10%)	Alternatyvų artumas, Ci (kai K1 *m* vertė - 10%)	Reitingas (kai K1 *m* vertė - 10%)
1	0.72	0.70	3	0.59	0.70	3
2	0.61	0.63	4	0.50	0.64	4
3	0.83	0.93	1	0.68	0.92	1
4	0.77	0.89	2	0.63	0.89	2
5	0.50	0.00	5	0.41	0.00	5

Kaip matoma, alternatyvų reitingas nepakito.

Antrojo kriterijaus (K2) svertinės vidurinės *m* vertės keitimo rezultatai:

39 lentelė. Fuzzy TOPSIS metodo jautrumo testavimas koreguojant K2 svertinę reikšmę m

Scenarijaus Nr.	Fuzzy trišalės normalizuotos svertinės vertės *m* svoris (kai K2 *m* vertė + 10%)	Alternatyvų artumas, Ci (kai K2 *m* vertė + 10%)	Reitingas (kai K2 *m* vertė + 10%)	Fuzzy trišalės normalizuotos svertinės vertės *m* svoris (kai K2 *m* vertė - 10%)	Alternatyvų artumas, Ci (kai K2 *m* vertė - 10%)	Reitingas (kai K2 *m* vertė - 10%)
1	0.71	0.70	3	0.58	0.69	3
2	0.62	0.64	4	0.51	0.64	4
3	0.71	0.93	1	0.58	0.92	1
4	0.57	0.89	2	0.47	0.90	2
5	0.43	0.00	5	0.35	0.00	5

Kaip matoma, alternatyvų reitingas taip pat nepakito.

Trečiojo kriterijaus (K3) svertinės vidurinės *m* vertės keitimo rezultatai:

40 lentelė. Fuzzy TOPSIS metodo jautrumo testavimas koreguojant K3 svertinę reikšmę m

Scenarijaus Nr.	Fuzzy trišalės normalizuotos svertinės vertės *m* svoris (kai K3 *m* vertė + 10%)	Alternatyvų artumas, Ci (kai K3 *m* vertė + 10%)	Reitingas (kai K3 *m* vertė + 10%)	Fuzzy trišalės normalizuotos svertinės vertės *m* svoris (kai K3 *m* vertė - 10%)	Alternatyvų artumas, Ci (kai K3 *m* vertė - 10%)	Reitingas (kai K3 *m* vertė - 10%)
1	0.54	0.69	3	0.44	0.70	3
2	0.59	0.64	4	0.48	0.64	4
3	0.69	0.93	1	0.56	0.92	1
4	0.69	0.89	2	0.56	0.89	2
5	0.44	0.00	5	0.36	0.00	5

Kaip matoma, alternatyvų reitingas nepakito.

Ketvirtojo kriterijaus (K4) svertinės vidurinės *m* vertės keitimo rezultatai:

41 lentelė. Fuzzy TOPSIS metodo jautrumo testavimas koreguojant K3 svertinę reikšmę m

Scenarijaus Nr.	Fuzzy trišalės normalizuotos svertinės vertės *m* svoris (kai K4 *m* vertė + 10%)	Alternatyvų artumas, Ci (kai K4 *m* vertė + 10%)	Reitingas (kai K4 *m* vertė + 10%)	Fuzzy trišalės normalizuotos svertinės vertės *m* svoris (kai K4 *m* vertė - 10%)	Alternatyvų artumas, Ci (kai K4 *m* vertė - 10%)	Reitingas (kai K4 *m* vertė - 10%)
1	0.72	0.70	3	0.62	0.70	3
2	0.61	0.64	4	0.52	0.64	4
3	0.78	0.92	1	0.67	0.93	1
4	0.83	0.89	2	0.71	0.89	2
5	0.44	0.00	5	0.38	0.00	5

Kaip matoma, alternatyvų reitingas vėl nepakito.

Penktojo kriterijaus (K5) svertinės vidurinės *m* vertės keitimo rezultatai:

42 lentelė. Fuzzy TOPSIS metodo jautrumo testavimas koreguojant K5 svertinę reikšmę m

Scenarijaus Nr.	Fuzzy trišalės normalizuotos svertinės vertės *m* svoris (kai K5 *m* vertė + 10%)	Alternatyvų artumas, Ci (kai K5 *m* vertė + 10%)	Reitingas (kai K5 *m* vertė + 10%)	Fuzzy trišalės normalizuotos svertinės vertės *m* svoris (kai K5 *m* vertė - 10%)	Alternatyvų artumas, Ci (kai K5 *m* vertė - 10%)	Reitingas (kai K5 *m* vertė - 10%)
1	0.40	0.69	3	0.33	0.71	3
2	0.58	0.64	4	0.47	0.64	4
3	0.62	0.92	1	0.51	0.93	1
4	0.71	0.89	2	0.58	0.89	2
5	0.36	0.00	5	0.29	0.00	5

Kaip matoma, alternatyvų reitingas nepakito.

Atlikta WASPAS ir Fuzzy TOPSIS metodų analizė pristatė, kad, Fuzzy TOPSIS metodas, lyginant su WASPAS metodu, yra mažiau jautrus pradinių įvesties duomenų pakeitimams - WASPAS metodo atveju pasirinktas ±5% kriterijų svorio pokytis, nes metodas jautrus mažiems svorio svyravimams. Tuo tarpu Fuzzy TOPSIS metodui taikytas ±10% pokytis, kadangi vertinant neapibrėžtomis (fuzzy) reikšmėmis reikšmingi skirtumai pasireiškia tik esant didesniam svorių pokyčiui. Todėl galima teigti, kad Fuzzy TOPSIS metodo naudojimas yra patikimas pasirinkimas panašaus pobūdžio tyrimams, ypač tuomet, kai įvesties duomenys stokoja tikslumo. Kalbant apie WASPAS metodo jautrumo analizės rezultatus, akivaizdu, kad šio tyrimo kontekste jis kelia gerokai daugiau rizikų jautrumo prasme, o jo praktinis panaudojimas turėtų būti apsvarstytas.

4. SIŪLOMO METODO VERIFIKAVIMAS

Skyriuje pristatomas verifikavimo eksperimentas, skirtas patikrinti naują saugumo reikalavimų kokybės lygio nustatymo metodą. Eksperimentas atliekamas lyginant dvi metodikas – naujai pasiūlytą daugiakriterį metodą ir tradicinį (nestruktūrizuotą) saugumo reikalavimų kokybės nustatymo metodą. Verifikavimo eksperimento tikslas - remiantis ekspertų nuomone, įvertinti naujai siūlomo daugiakriterio metodo veikimą patikimumo, pritaikomumo, sugaišto laiko ir efektyvumo aspektais. Galiausiai, tikslas bus pasiektas, kai abiejų metodų taikymo rezultatai bus palyginti tarpusavyje.

Eksperimento atlikimo metu kliaunamasi 8 ekspertų nuomonėmis, šie ekspertai yra iš pradinės ekspertų grupės. Pirmieji 4 iš 8 ekspertų vertins registrų ir informacinių sistemų specifikacijų saugumo reikalavimus (scenarijus) (žr. 3.2.3. skyrelis) vadovaudamiesi naujai pasiūlytu daugiakriteriu metodu saugumo reikalavimų kokybei nustatyti (žr. 4 priedas), likusieji 4 ekspertai minėtus scenarijus vertins naudodami tradicinį (nestruktūrizuotą) vertinimo metodą (žr. 5 priedas).

Toliau yra pristatomi ekspertinio vertinimo rezultatai, kuomet ekspertai scenarijų įvertinimui naudoto tradicinį (nestruktūrizuotą) saugumo reikalavimų kokybės nustatymo metodą (žr. 43 lentelė).

43 lentelė. Ekspertų įvertinimai scenarijams taikant tradicinį saugumo reikalavimų kokybės lygį įvertinantį metodą

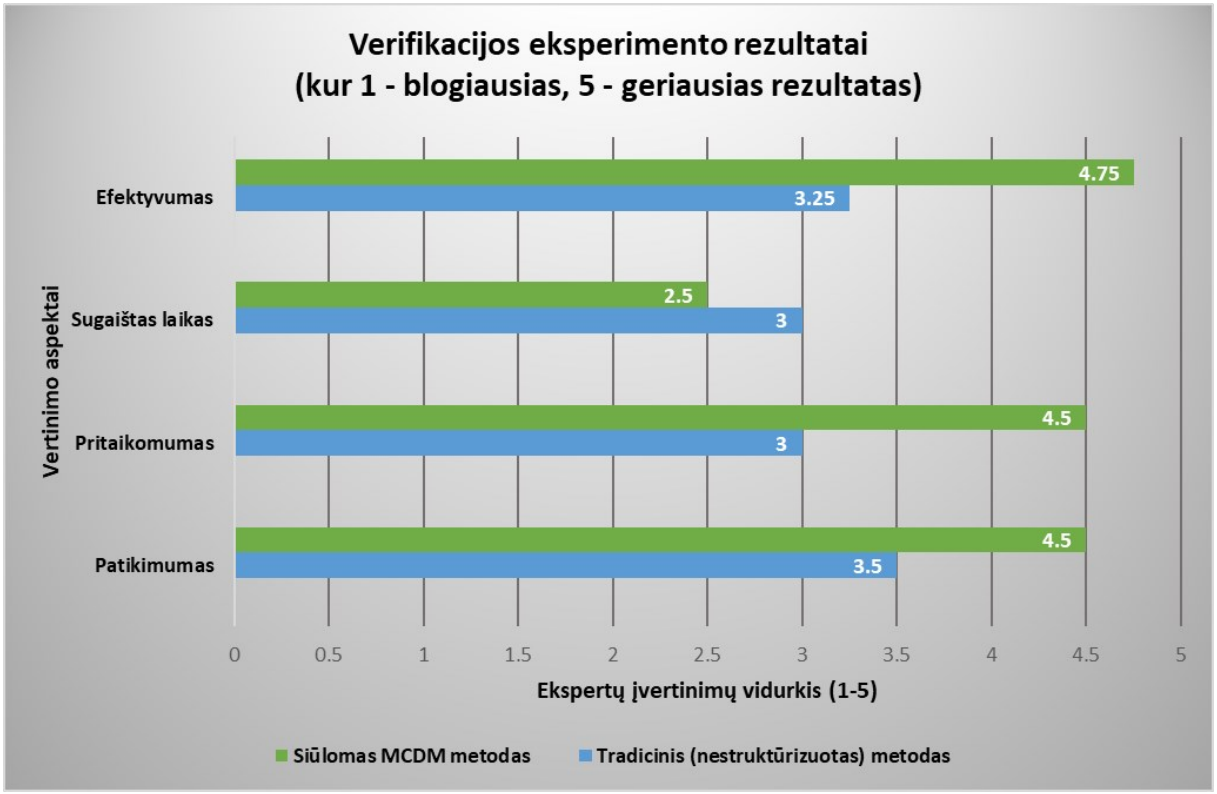
Ekspertas / *Scenarijus*	***E3***	***E4***	***E5***	***E9***	***Reitingas***
1 (KDR)	3	2	4	2	4
2 (MR)	5	5	5	4	1
3 (VIPVIS)	3	3	3	3	5
4 (PTR)	4	4	2	3	3
5 (NTIS)	2	3	4	5	2

Tarpusavyje lyginant scenarijams ekspertų priskirtus įvertinimus, kuomet buvo naudojamas naujas daugiakriteris metodas ir tradicinis (nestruktūrizuotas) vertinimo metodas, rezultatai kardinaliai išsiskyrė. Tikėtina, kad išsiskyrimus, taikant tradicinį (nestruktūrizuotą) vertinimo metodą, galėjo lemti ekspertų vertinimo nuoseklumo stoka, aiškios vertinimo struktūros neturėjimas (vertinimas „iš akies“ be aiškių kriterijų) bei fragmentiškumas. Šie aspektai gali neigiamai įtakoti visą vertinimo procesą bei galutinį sprendimo priėmimą.

Po vertinimų atlikimo, ekspertams buvo pateikti keli klausimai, siekiant nustatyti, kuris, jų nuomone, iš registrų ir informacinių sistemų specifikacijų saugumo reikalavimų kokybės lygį įvertinančių metodų yra pranašesnis patikimumo, pritaikomumo, sugaišto laiko ir efektyvumo prasme. Klausimų formuluotės yra pateikiamos toliau:

1. Penkiabalėje skalėje (1–5) įvertinkite, kiek jūsų naudoto metodo rezultatai yra patikimi ir leidžia priimti pagrįstą, logišką sprendimą, įvertinant saugumo reikalavimų kokybės lygį (kai 1 – visiškai nepatikimi, 5 – visiškai patikimi ir pagrįsti).
2. Penkiabalėje skalėje (1–5) įvertinkite, kiek jūsų naudotas metodas yra lankstus ir pritaikomas skirtingoms specifikacijų saugumo reikalavimų apibrėžtims, siekiant įvertinti jų kokybės lygį (kai 1 – labai ribotas, 5 – itin lankstus ir pritaikomas).
3. Penkiabalėje skalėje (1–5) įvertinkite, kiek laiko buvo sugaišta taikant jūsų naudotą metodą saugumo reikalavimų kokybės lygiui įvertinti (kai 1 – didžiausios laiko sąnaudos, 5 – mažiausios laiko sąnaudos).
4. Penkiabalėje skalėje (1-5) įvertinkite, kiek jūsų taikytas metodas buvo efektyvus, nustatant saugumo reikalavimų kokybės lygį (kai 1 – prasčiausias efektyvumą nusakantis įvertis, 5 – geriausias efektyvumą nusakantis įvertis).

Gavus ekspertų atsakymus į pateiktus klausimus, jie pristatomi grafiškai (žr. 8 pav.):



8 pav. Ekspertų įvertinimų pasiskirstymas verifikacijos eksperimento metu

Ekspertų vertinimo rezultatai pristatė, kad naujas siūlomas MCDM metodas yra pranašesnis už tradicinį (nestruktūrizuotą) metodą efektyvumo, pritaikomumo bei patikimumo prasmėmis. Deja, tačiau įžvelgiama viena MCDM silpnybė - ekspertų vertinimu, sugaišto laiko sąnaudos, lyginant su tradiciniu (nestruktūrizuotu) vertinimo metodu, buvo šiek tiek didesnės. Tai būtų galima paaiškinti tuo, kad tradiciniame (nestruktūrizuotame) metode nėra naudojama struktūrizuota bei nuosekli vertinimo metodika, kitaip tariant, vertinimai atliekami pagal intuiciją.

IŠVADOS

1. Atlikus registrų ir informacinių sistemų saugumo reikalavimų ir jų kokybės gerinimo analizę paaiškėjo, kad nagrinėtų šaltinių autoriai siūlo platų įvairių funkcinių ir nefunkcinių reikalavimų taikymą saugumui užtikrinti; saugumo reikalavimų kokybės atributai kaip aiškumas, išsamumas, korektiškumas yra būtini sėkmingų projektų įgyvendinimui; tinkamas daugiakriterių sprendimo metodų (MCDM) pasirinkimas yra itin svarbus, o konkretaus metodo taikymo poreikis yra įvertinamas individualiai;
2. Darbe aprašyta kriterijais grįsta lyginamojo vertinimo metodika, kuria galima įvertinti saugumo reikalavimų kokybę, taikant daugiakriterius metodus. AHP ir „Fuzzy“ TOPSIS metodu apskaičiuojamas kriterijų reikšmingumas (svorių reikšmės); naudojant WASPAS su „Fuzzy“ TOPSIS galima nustatyti saugumo reikalavimų kokybės lygį specifikacijos kontekste. AHP padeda kriterijų svorio nustatymo procese, atkreipiant dėmesį į sprendžiamos problemos svarbą; WASPAS metodas įtraukia daugelio kriterijų vertinimo metodus, tai suteikia galimybę tiksliai nustatyti saugumo reikalavimų kokybės lygį. „Fuzzy“ TOPSIS metodas suteikia alternatyvų koreliacijos galimybę, atkreipiant dėmesį į neapibrėžtumą ir subjektyvias ekspertų nuomones. Sėkmingas metodų naudojimas užtikrina, kad vertinimo procesas būtų kokybiškas, patikimas ir lankstus.
3. Siūlomo naujo daugiakriterio metodo eksperimentinio vertinimo pirmame tyrimo etape ekspertai identifikavo penkis kriterijus, kurie, jų nuomone, labiausiai tinkami atliekant registrų ir informacinių sistemų specifikacijose apibrėžiamų saugumo reikalavimų kokybės vertinimą; Antrame etape ekspertai taikė AHP ir „Fuzzy“ TOPSIS metodus kriterijų svertinėms reikšmėms nustatyti; Trečiame etape ekspertai atliko saugumo reikalavimų vertinimą, priskiriant kiekybines WASPAS ir kokybines „Fuzzy“ TOPSIS reikšmes alternatyvoms. Tolesnė tyrimo praktinė eiga susidarė iš skaičiavimų WASPAS ir „Fuzzy“ TOPSIS metodais atlikimo, siekiant nustatyti saugumo reikalavimų rinkinių kokybės reitingą. Apskaičiuotas ekspertų tarpusavio nuomonių suderinamumo rodiklis w siekia 0.69 – tai leidžia teigti, kad ekspertus vienija stiprus sutarimas. Galiausiai, atlikta daugiakriterių metodų jautrumo analizė pristatė, kad WASPAS metodas, lyginant su „Fuzzy“ TOPSIS, yra kur kas jautresnis pradinių duomenų pasikeitimams.
4. Siekiant įsitikinti, kad siūlomas naujas daugiakriteris metodas yra tinkamas registrų ir informacinių sistemų specifikacijų saugumo reikalavimų kokybės vertinimui, buvo atliktas metodo verifikavimas. Eksperimento vykdymo metu 8 ekspertų grupė buvo padalyta į dvi, lygias grupes – 4 ekspertai saugumo reikalavimų kokybės vertinimą

atliko taikydami tradicinį (nestruktūrizuotą) vertinimo metodą, o likusieji 4 ekspertai kokybės vertinimą atliko vadovaudamiesi naujo daugiakriterio metodo metodika. Iš ekspertų gauti vertinimo rezultatai pristatė, kad MCDM metodas yra pranašesnis už tradicinį (nestruktūrizuotą) metodą efektyvumo (4.75 prieš 3.25), pritaikomumo (4.5 prieš 3) bei patikimumo (4.5 prieš 3.5) aspektais. Ekspertai vertinimo metu identifikavo vieną siūlomo daugiakriterio metodo trūkumą – laiko sąnaudas, jos nežymiai didesnės už tradicinio (nestruktūrizuoto) metodo sąnaudas (3 prieš 2.5). Toks ekspertų vertinimas motyvuojamas tuo, kad tradiciniame metode nėra naudojama struktūrizuota ar nuosekli vertinimo metodika. Pasiūlytas MCDM metodas likviduoja tradiciniam vertinimo metodui būdingas spragas: nenuoseklumą, struktūriškumo, patikimumo bei fragmentiškumo stoką, todėl tokiu būdu patobulinamas saugumo reikalavimų kokybės vertinimas.

LITERATŪROS SĄRAŠAS

Alamoodi, A. H., Zaidan, B. B., Albahri, O. S., Garfan, S., Ahmaro, I. Y. Y., Mohammed, R. T., Zaidan, A. A., Ismail, A. R., Albahri, A. S., Momani, F., Al-Samarraay, M. S., Jasim, A. N., & R.Q.Malik. (2023). Systematic review of MCDM approach applied to the medical case studies of COVID-19: trends, bibliographic analysis, challenges, motivations, recommendations, and future directions. *Complex & Intelligent Systems*, *9*(4), 4705–4731. https://doi.org/10.1007/s40747-023-00972-1

Alencar, G. A., De S. Oliveira, F. V., Da Silva Correia-Neto, J., & Teixeira, M. M. (2019). Non-Functional Requirements In Health Information Systems: *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–5. https://doi.org/10.23919/CISTI.2019.8760720

Altersoft. (2023). *Functional and Nonfunctional Requirements: Specification and Types*. https://www.altexsoft.com/blog/functional-and-non-functional-requirements-specification-and-types/

Ananda, J., & Herath, G. (2009). A critical review of multi-criteria decision making methods with special reference to forest management and planning. *Ecological Economics*, *68*(10), 2535–2548. https://doi.org/10.1016/j.ecolecon.2009.05.010

Andriusaitiene, D., Gineviciene, V. B., & Sileika, A. (2008). Daugiakriterinis profesinio mokymo kokybes valdymo vertinimo modelis. *Verslas: teorija ir praktika*, *9*(2), 88–96. https://doi.org/10.3846/1648-0627.2008.9.88-96

Badalpur, M., & Nurbakhsh, E. (2021). An application of WASPAS method in risk qualitative analysis: a case study of a road construction project in Iran. *International Journal of Construction Management*, *21*(9), 910–918. https://doi.org/10.1080/15623599.2019.1595354

Blake, J. N., Kerr, D. V., & Gammack, J. G. (2016). Streamlining patient consultations for sleep disorders with a knowledge-based CDSS. *Information Systems*, *56*, 109–119. https://doi.org/10.1016/j.is.2015.08.003

Chakraborty, S., & Zavadskas, E. K. (2014). Applications of WASPAS Method in Manufacturing Decision Making. *Informatica*, *25*(1), 1–20. https://doi.org/10.15388/Informatica.2014.01

Chung, L., & do Prado Leite, J. C. S. (2009). *On Non-Functional Requirements in Software Engineering* (p. 363–379). https://doi.org/10.1007/978-3-642-02463-4_19

Dymova, L., Sevastjanov, P., & Tikhonenko, A. (2013). An approach to generalization of fuzzy TOPSIS method. *Information Sciences*, *238*, 149–162. https://doi.org/10.1016/j.ins.2013.02.049

Ginevičius, R., Zubrecovas, V., & Ginevičius, T. (2009). Nekilnojamojo turto investicinių projektų efektyvumo vertinimo metodikos. *Verslas: teorija ir praktika*, *10*(3), 181–190. https://doi.org/10.3846/1648-0627.2009.10.181-190

Gómez-Martínez, E., Linaje, M., Sánchez-Figueroa, F., Iglesias-Pérez, A., Preciado, J. C., González-Cabero, R., & Merseguer, J. (2015). A semantic approach for designing Assistive Software Recommender systems. *Journal of Systems and Software*, *104*, 166–178. https://doi.org/10.1016/j.jss.2015.03.009

Hadjidimitriou, S., Charisis, V., Kyritsis, K., Konstantinidis, E., Delopoulos, A., Bamidis, P., Bostantjopoulou, S., Rizos, A., Trivedi, D., Chaudhuri, R., Klingelhoefer, L., Reichmann, H., Wadoux, J., De Craecker, N., Karayiannis, F., Fagerberg, P., Ioakeimidis, I., Stadtschnitzer, M., Esser, A., … Hadjileontiadis, L. J. (2016). Active and healthy ageing for Parkinson's disease patients' support: A user's perspective within the i-PROGNOSIS framework. *2016 1st International Conference on Technology and Innovation in Sports, Health and Wellbeing (TISHW)*, 1–8. https://doi.org/10.1109/TISHW.2016.7847785

Heck, P., & Zaidman, A. (2018). A systematic literature review on quality criteria for agile requirements specifications. *Software Quality Journal*, *26*(1), 127–160. https://doi.org/10.1007/s11219-016-9336-4

International Organization for Standardization. (1999). *Information technology — Programming languages — Ada: Conformity assessment of a language processor. (Standard No. ISO/IEC 18009:1999)*. https://www.iso.org/standard/31051.html

International Organization for Standardization. (2008). *Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®) (Standard No. ISO/IEC 21827:2008)*. https://www.iso.org/standard/44716.html

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security - Part 2: Security functional components (Standard No. ISO/IEC 15408-2:2022)*. https://www.iso.org/standard/72892.html

International Organization for Standardization. (2023). *Industrial automation systems and integration — Integration of life-cycle data for process plants including oil and gas production facilities — Part 11: Simplified industrial usage of reference data based*

on RDFS methodology (Standard No. ISO/TS 15926-11:2023). https://www.iso.org/standard/79005.html

Kolios, A., Mytilinou, V., Lozano-Minguez, E., & Salonitis, K. (2016). A Comparative Study of Multiple-Criteria Decision-Making Methods under Stochastic Inputs. *Energies*, *9*(7), 566. https://doi.org/10.3390/en9070566

Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas. (2023). *Valstybės žinios*. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/0f777342a48b11ee8172b53a675305ab?jfwid=p1kf1mbtj

Mark Velasquez, & Patrick Thomas Hester. (2013). *An analysis of multi-criteria decision making methods*. *10*, 56–66.

Mellado, D., Blanco, C., Sánchez, L. E., & Fernández-Medina, E. (2010). A systematic review of security requirements engineering. *Computer Standards & Interfaces*, *32*(4), 153–165. https://doi.org/10.1016/j.csi.2010.01.006

Michiel Meulendijk, E.A. Meulendijks, P.A.F. Jansen, Mattijs E Numans, & Marco Spruit. (2014). *What concerns users of medical apps? Exploring non-functional requirements of medical mobile applications*. https://www.researchgate.net/publication/286060117_What_concerns_users_of_medical_apps_Exploring_non-functional_requirements_of_medical_mobile_applications

Mokhtarian, M. N. (2015). A note on "Extension of fuzzy TOPSIS method based on interval-valued fuzzy sets". *Applied Soft Computing*, *26*, 513–514. https://doi.org/10.1016/j.asoc.2014.10.013

Montgomery, L., Fucci, D., Bouraffa, A., Scholz, L., & Maalej, W. (2022). Empirical research on requirements quality: a systematic mapping study. *Requirements Engineering*, *27*(2), 183–209. https://doi.org/10.1007/s00766-021-00367-z

Moslem, S., Ghorbanzadeh, O., Blaschke, T., & Duleba, S. (2019). Analysing Stakeholder Consensus for a Sustainable Transport Development Decision by the Fuzzy AHP and Interval AHP. *Sustainability*, *11*(12), 3271. https://doi.org/10.3390/su11123271

NLP asociacija. (2014). *Tyrimo „Socialinio ugdymo srityje dirbančių tyrėjų trūkstamų kompetencijų identifikavimas" ataskaita*. http://www.esparama.lt/es_parama_pletra/failai/ESFproduktai/2014_Tyrimo_ataskaita.pdf

Pekar, V., Felderer, M., & Breu, R. (2014). Improvement Methods for Software Requirement Specifications: A Mapping Study. *2014 9th International Conference*

on the Quality of Information and Communications Technology, 242–245. https://doi.org/10.1109/QUATIC.2014.40

Pereira, T., Alencar, F., Silva, J., & Castro, J. (2013). Requisitos Não-Funcionais em Modelos de Processos de Negócio: Uma Revisão Sistemática. *Anais do IX Simpósio Brasileiro de Sistemas de Informação (SBSI 2013)*, 37–48. https://doi.org/10.5753/sbsi.2013.5674

Poškas, G., Poškas, P., Sirvydas, A., & Šimonis, A. (2012). Daugiakriterinės analizės metodo taikymas parenkant Ignalinos AE V1 pastato įrengimų išmontavimo būdą. 2. Daugiakriterinės analizės metodika ir jos taikymo rezultatai. *Energetika*, *58*(2). https://doi.org/10.6001/energetika.v58i2.2341

Sahoo, S. K., & Goswami, S. S. (2023). A Comprehensive Review of Multiple Criteria Decision-Making (MCDM) Methods: Advancements, Applications, and Future Directions. *Decision Making Advances*, *1*(1), 25–48. https://doi.org/10.31181/dma1120237

Siksnelyte-Butkiene, I., Zavadskas, E. K., & Streimikiene, D. (2020). Multi-Criteria Decision-Making (MCDM) for the Assessment of Renewable Energy Technologies in a Household: A Review. *Energies*, *13*(5), 1164. https://doi.org/10.3390/en13051164

Simanavičienė, R. (2011). *Kiekybinių daugiatikslių sprendimo priėmimo metodų jautrumo analizė*. Vilnius Gediminas Technical University. https://doi.org/10.20334/1973-M

Taherdoost, H., & Madanchian, M. (2023). Multi-Criteria Decision Making (MCDM) Methods and Concepts. *Encyclopedia*, *3*(1), 77–87. https://doi.org/10.3390/encyclopedia3010006

Triantafyllidis, A., Velardo, C., Chantler, T., Shah, S. A., Paton, C., Khorshidi, R., Tarassenko, L., & Rahimi, K. (2015). A personalised mobile-based home monitoring system for heart failure: The SUPPORT-HF Study. *International Journal of Medical Informatics*, *84*(10), 743–753. https://doi.org/10.1016/j.ijmedinf.2015.05.003

Visure. (s.a.). *What are Functional Requirements: Examples, Definition, Complete Guide*. https://visuresolutions.com/blog/functional-requirements/

Wang, P., Zhu, Z., & Wang, Y. (2016). A novel hybrid MCDM model combining the SAW, TOPSIS and GRA methods based on experimental design. *Information Sciences*, *345*, 27–45. https://doi.org/10.1016/j.ins.2016.01.076

Zavadskas, E. K., Turskis, Z., & Antucheviciene, J. (2012a). Optimization of Weighted Aggregated Sum Product Assessment. *Electronics and Electrical Engineering*, *122*(6). https://doi.org/10.5755/j01.eee.122.6.1810

Zavadskas, E. K., Turskis, Z., & Antucheviciene, J. (2012b). Optimization of Weighted Aggregated Sum Product Assessment. *Electronics and Electrical Engineering*, *122*(6). https://doi.org/10.5755/j01.eee.122.6.1810

PRIEDAI

1 priedas. Esminių kriterijų identifikavimas

Pateikiama ekspertinės apklausos forma, kurios tikslas – išskirti *penkis* (5) esminius kriterijus, atliekant registro ir (ar) informacinės sistemos specifikacijos validaciją.

Užduotis: pasirinkti (arba eksperto nuožiūra išskirti atsakymų sekcijoje) *penkis* (5), eksperto manymu, svarbiausius kriterijus, nustatant registro ir (ar) informacinės sistemos specifikacijos reikalavimų kokybę. Pageidautina kriterijus identifikuoti remiantis jų teikiama svarba ir įtaka specifikacijose apibrėžtiems saugumo reikalavimams.

Eiga: iš toliau pateikto sąrašo pasirinkite (arba savo nuožiūra išskirkite) *penkis* (5) kriterijus, o pasirinkimo varianto žymėjimą (arba savo pasiūlymą) nurodykite apačioje esančiame galutinio atsakymo laukelyje.

a) Kriptografijos palaikymo išsamumas
b) Vartotojų identifikacijos ir autentifikacijos aktualumas
c) Sistemos architektūros integracijos išsamumas
d) Papildomų saugumo priemonių korektiškumas
e) Saugumo įvykių registravimo nepertekliškumas
f) Atitikimo tarptautiniams standartams nedviprasmiškumas
g) Atkūrimo po saugumo sutrikimų išbaigtumas
h) Atsparumo prieinamumo išpuoliams nepertekliškumas
i) Prieigos kontrolės politikos nuoseklumas
j) Atitikties teisinei ir reguliacinei sistemai išsamumas
k) Saugos priemonių parinkimo principų korektiškumas
l) Duomenų konfidencialumo užtikrinimo aiškumas

Ekspertinio vertinimo metu ekspertai pasiūlė šiuos papildomus kriterijus:

m) Vartotojų identifikacijos ir autentifikacijos korektiškumas
n) Prieigos kontrolės politikos aiškumas

Jūsų pasirinkti (pasiūlyti) atsakymai:

2 priedas. Kriterijų svorių bei svarbos nustatymas (AHP)

Pateikiama ekspertinės apklausos forma, kurios tikslas – ekspertų identifikuotiems kriterijams nustatyti svorius bei įvertinti jų tarpusavio svarbą.

Užduotis: nustatyti, eksperto manymu, kiekvieno iš kriterijų tarpusavio svarbą, įvertinant jų svorį atitinkama skaitine reikšme.

Eiga: remiantis 1 lentelėje pateiktais išskirtais kriterijais, atlikite jų tarpusavio svorių bei svarbos nustatymą 3 lentelėje. Naudojantis pateikta vertinimo metodika 2 lentelėje, atlikite kriterijų svorių nustatymą nurodydami skaitinę reikšmę 3 lentelės stulpelyje pavadinimu „Svoris pagal reitingą (1-9)“, tuomet toje pačioje lentelėje, šalimais esančiame stulpelyje „Kuris kriterijus svarbesnis? (K)“, nurodykite, kuris kriterijus (iš dviejų toje eilutėje nurodytų) yra svarbesnis.

Vertinamųjų (lyginamųjų) kriterijų sąrašas

Išskirto kriterijaus pavadinimas	***Kriterijaus žymėjimas***
Vartotojų identifikacijos ir autentifikacijos aktualumas	K1
Prieigos kontrolės politikos nuoseklumas	K2
Atkūrimo po saugumo sutrikimų išbaigtumas	K3
Duomenų konfidencialumo užtikrinimo aiškumas	K4
Atitikties teisinei ir reguliacinei sistemai išsamumas	K5

Vertinimo (lyginimo) metodika

Skalė (reitingas)	***Reitingavimo paaiškinimas***
1	Kriterijų svarba yra vienoda (lygi)
3	Kriterijaus pranašumas lyginant su alternatyva - vidutinis
5	Kriterijaus pranašumas lyginant su alternatyva – stiprus
7	Kriterijaus pranašumas lyginant su alternatyva – labai stiprus
9	Kriterijaus pranašumas lyginant su alternatyva – absoliutus

2, 4, 6, 8	Kompromisinės tarpinės reikšmės tarp dviejų gretimų sprendimų

Kriterijų porinis palyginimas (AHP metodas)

Pirmasis kriterijus	***Antrasis kriterijus***	***Kuris kriterijus svarbesnis? (K)***	***Svoris pagal reitingą (1-9)***
Vartotojų identifikacijos ir autentifikacijos aktualumas (K1)	Prieigos kontrolės politikos nuoseklumas (K2)		
Vartotojų identifikacijos ir autentifikacijos aktualumas (K1)	Atkūrimo po saugumo sutrikimų išbaigtumas (K3)		
Vartotojų identifikacijos ir autentifikacijos aktualumas (K1)	Duomenų konfidencialumo užtikrinimo aiškumas (K4)		
Vartotojų identifikacijos ir autentifikacijos aktualumas (K1)	Atitikties teisinei ir reguliacinei sistemai išsamumas (K5)		
Prieigos kontrolės politikos nuoseklumas (K2)	Atkūrimo po saugumo sutrikimų išbaigtumas (K3)		
Prieigos kontrolės politikos nuoseklumas (K2)	Duomenų konfidencialumo užtikrinimo aiškumas (K4)		
Prieigos kontrolės politikos nuoseklumas (K2)	Atitikties teisinei ir reguliacinei sistemai išsamumas (K5)		

Atkūrimo po saugumo sutrikimų išbaigtumas (K3)	Duomenų konfidencialumo užtikrinimo aiškumas (K4)		
Atkūrimo po saugumo sutrikimų išbaigtumas (K3)	Atitikties teisinei ir reguliacinei sistemai išsamumas (K5)		
Duomenų konfidencialumo užtikrinimo aiškumas (K4)	Atitikties teisinei ir reguliacinei sistemai išsamumas (K5)		

3 priedas. Kriterijų svarbos nustatymas (*Fuzzy* TOPSIS)

Pateikiama ekspertinės apklausos forma, kurios tikslas – priskirti **lingvistines** reikšmes ankstesnio vertinimo metu išskirtiems kriterijams.

Užduotis: nustatyti, eksperto manymu, kiekvieno iš kriterijų svarbą, įvertinant jų svorį atitinkama **lingvistine** reikšme. Pageidautina vertinimą atlikti remiantis kiekvieno kriterijaus teikiama svarba registrų ir (ar) informacinių sistemų specifikacijų saugumo reikalavimų kokybės validacijos procese.

Eiga: vadovaudamiesi 1 lentelėje pateiktu lingvistinių reikšmių (terminų) ir sutrumpinimų sąrašu, atlikite išskirtų kriterijų svarbos nustatymą 2 lentelėje esančiame stulpelyje „Priskirta lingvistinė reikšmė“. Jame priskirkite lingvistinės reikšmės sutrumpinimą, pvz., „Vidutinis“ – V.

Lingvistinių reikšmių (terminų) ir sutrumpinimų sąrašas

Lingvistinė reikšmė (terminas)	***Lingvistinės reikšmės sutrumpinimas***
Labai žemas	LŽ
Žemas	Ž
Vidutinis	V
Aukštas	A
Labai aukštas	LA

Kriterijų lingvistinių reikšmių priskyrimo lentelė

Išskirtas kriterijus	***Priskirta lingvistinė reikšmė***
Vartotojų identifikacijos ir autentifikacijos aktualumas (K1)	
Prieigos kontrolės politikos nuoseklumas (K2)	
Atkūrimo po saugumo sutrikimų išbaigtumas (K3)	
Duomenų konfidencialumo užtikrinimo aiškumas (K4)	

Atitikties teisinei ir reguliacinei sistemai išsamumas (K5)	

4 priedas. Specifikacijų saugumo reikalavimų analizė ir vertinimas

Pateikiama ekspertinės apklausos forma, kurios tikslas – įvertinti skirtingus reikalavimų sąrašus (scenarijus), priskiriant jiems atitinkamas skaitines reikšmes.

Užduotis: nustatyti, eksperto manymu, kiekvieno reikalavimų sąrašo (scenarijaus) individualių saugumo reikalavimų atitikimą anksčiau identifikuotiems kriterijams, įvertinant atitikimą specifine skaitine reikšme.

Eiga: 1 lentelėje yra pateikiami anksčiau ekspertų išskirti kriterijai. Remdamiesi šiais kriterijais, atlikite 4, 5, 6, 7 ir 8 lentelėse pateiktų reikalavimų individualų vertinimą 3 lentelėje. Vertinimo metodika apima skalę nuo 1 iki 5, detalesnė metodinė informacija ir vertinimo pavyzdžiai yra pateikiami 2 lentelėje. Atskiras vertinimo pavyzdys ir instrukcija yra pateikiami dokumento pabaigoje.

Dėmesio! ***Scenarijuose pateikti reikalavimai yra išdėstyti atsitiktine tvarka, o vieno reikalavimo apimamas spektras kriterijų atžvilgiu gali varijuoti. Pvz., vienas reikalavimas gali būti susijęs su keliais kriterijais, o kitas reikalavimas – tik su vienu kriterijumi, tačiau kiekviename scenarijuje yra bent po vieną reikalavimą atitinkamam kriterijui.***

Anksčiau identifikuotų kriterijų sąrašas, kriterijų žymėjimas bei kokybės atributų paaiškinimas

Ekspertų išskirto kriterijaus pavadinimas	***Kriterijaus kokybės atributo paaiškinimas***	***Kriterijaus žymėjimas***
Vartotojų identifikacijos ir autentifikacijos aktualumas	Aktualumas - reikalavimas turi būti aktualus taikomai sistemai ir atitikti jos numatytus poreikius;	K1
Prieigos kontrolės politikos nuoseklumas	Nuoseklumas - reikalavimas turi derėti su kitais sistemos saugumo reikalavimais ir būti integruotas;	K2
Atkūrimo po saugumo sutrikimų išbaigtumas	Išbaigtumas - reikalavimas turi turėti visas būtinas sudedamąsias dalis;	K3
Duomenų konfidencialumo užtikrinimo aiškumas	Aiškumas - reikalavimas yra suformuluotas tiksliai, vengiant abstrakčių ar neaiškių terminų	K4
Atitikties teisinei ir reguliacinei sistemai išsamumas	Išsamumas - reikalavimas turi pakankamai apimti	K5

Ekspertų išskirto kriterijaus pavadinimas	*Kriterijaus kokybės atributo paaiškinimas*	*Kriterijaus žymėjimas*
	aspektus, kuriems jis yra skirtas	

Saugumo reikalavimų vertinimo skalė ir pavyzdžiai pagal identifikuotų kriterijų sąrašą

<table>
<tr><th>Kriterijaus pavadinimas</th><th>Kriterijų apibūdinantys klausimai, pvz.,</th><th>Vertinimo skalė, parametro apibūdinimas + pavyzdys</th></tr>
<tr><td>Vartotojų identifikacijos ir autentifikacijos aktualumas (K1)</td><td>•Ar apibrėžtas tapatybės patvirtinimo (autentifikavimo) mechanizmas (pvz., slaptažodis, biometrika, PIN, 2FA, MFA) atitinka keliamus saugumo poreikius?
•Ar vartotojai sistemoje yra unikalūs ir identifikuojami pagal aktualiai apibrėžtą identifikatorių (pvz., prisijungimo vardą, naudotojo ID)?</td><td>
<table>
<tr><th>Įvertis</th><th>Aprašymas</th><th>Reikalavimo pvz.,</th></tr>
<tr><td>5</td><td>Identifikacija ir autentifikacija atitinka sistemos poreikius</td><td>„Naudotojai atpažįstami, naudojama prisijungimo vardų, slaptažodžių ir prieigos teisių sistema, derinama su kelių faktorių autentifikacija bei naudotojų veiksmų stebėsena realiu laiku“</td></tr>
<tr><td>4</td><td>Identifikacija ir autentifikacija pritaikyta sistemos poreikiams, galima optimizacija</td><td>„Naudotojai turi būti atpažįstami, patikrinami 2FA, jų prieiga valdoma naudojant prisijungimo vardus, slaptažodžius ir prieigos teisių sistemą“, - tačiau dar galėtų veikti prisijungimų stebėsena</td></tr>
<tr><td>3</td><td>Identifikacija egzistuoja, bet nėra optimaliai integruota su autentifikacija</td><td>„Naudotojai turi būti atpažįstami prisijungimo vardu ir slaptažodžiu“, - tačiau autentifikacija atliekama tik vienu ir tuo pačiu veiksniu</td></tr>
<tr><td>2</td><td>Identifikacija nepakankama arba autentifikacija per silpna ar perteklinė</td><td>„Prisijungimo vardų ir slaptažodžių sistema naudojama darbuotojų tapatybei nustatyti“, - tačiau nėra aiškaus mechanizmo, kaip patikrinami naudotojai</td></tr>
<tr><td>1</td><td>Identifikacija prasta arba neegzistuojanti, autentifikacija per silpna</td><td>„Naudotojai turi būti atpažįstami“, - tačiau nėra jokių mechanizmų, leidžiančių identifikuoti naudotojus ar patikrinti jų tapatybę</td></tr>
</table>
</td></tr>
<tr><td>Prieigos kontrolės politikos</td><td>•Ar apibrėžti prieigos kontrolės reikalavimai yra pakankamai</td><td>
<table>
<tr><th>Įvertis</th><th>Aprašymas</th><th>Reikalavimo pvz.,</th></tr>
<tr><td>5</td><td>Politika pilnai</td><td>„Naudotojai negali atlikti operacijų tiesiai</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Kriterijaus pavadinimas</th><th>Kriterijų apibūdinantys klausimai, pvz.,</th><th colspan="3">Vertinimo skalė, parametro apibūdinimas + pavyzdys</th></tr>
<tr><td>nuoseklumas (K2)</td><td>integruoti (ar dera bendrame saugumo kontekste)?
•Ar prieigos kontrolės politikos taisyklės yra taikomos visiems vartotojams, įskaitant ir administratorius?</td><td></td><td>suderinta su saugumo nuoseklumo poreikiais</td><td>duomenų bazėje, priėjimas prie duomenų ribojamas teisių ir rolių pagalba, taip pat priėjimas ribojamas fiksuotais naudotojais; DB administratorius neturi prieigos prie duomenų failų be OS leidimo, vykdomas nuolatinis auditas“</td></tr>
<tr><td></td><td></td><td>4</td><td>Politika nuosekliai apibrėžta, bet gali būti tobulinama</td><td>„Naudotojai negali atlikti operacijų tiesiai duomenų bazėje, priėjimas prie duomenų ribojamas teisių ir rolių pagalba, taip pat priėjimas ribojamas fiksuotais naudotojais“, - bet nėra automatizuotos teisių (rolių) peržiūros</td></tr>
<tr><td></td><td></td><td>3</td><td>Prieigos kontrolė egzistuoja, bet yra neatitikimų</td><td>„Naudotojai negali turėti galimybės atlikti operacijų tiesiai duomenų bazėje, priėjimas prie duomenų ribojamas teisių ir rolių pagalba“, - tačiau be sisteminių vartotojų integracijos</td></tr>
<tr><td></td><td></td><td>2</td><td>Yra prieigos apribojimai, bet jie nevisiškai įgyvendinti</td><td>„Naudotojai negali atlikti operacijų tiesiai duomenų bazėje, tačiau DB administratoriai gali pasiekti duomenų failus be OS apribojimų“ – ribojimai taikomi, tačiau yra spragų</td></tr>
<tr><td></td><td></td><td>1</td><td>Prieigos valdymas nėra deramai apibrėžtas arba yra nesaugus</td><td>„Naudotojai gali atlikti operacijas tiesiai duomenų bazėje“, - nesilaikoma prieigos kontrolės principų</td></tr>
<tr><td>Atkūrimo po saugumo sutrikimų išbaigtumas (K3)</td><td>•Ar yra įdiegtos automatinės atkūrimo priemonės gedimo atvejais?
•Ar apibrėžti atkūrimo po saugumo sutrikimų reikalavimai turi visas būtinas sudedamąsias dalis?</td><td>Įvertis</td><td>Aprašymas</td><td>Reikalavimo pvz.,</td></tr>
<tr><td></td><td></td><td>5</td><td>Visiškai automatizuotas atkūrimo mechanizmas, kuris apima daugelį galimų sutrikimų ir turi visas sudedamąsias dalis</td><td>„Sistema turi užtikrinti korektišką avarinių saugumo situacijų valdymą (pvz., NIST, SANS), rodyti atitinkamus avarinius pranešimus ir visiškai automatiškai grįžti į pradinę būklę be naudotojo įsikišimo“</td></tr>
<tr><td></td><td></td><td>4</td><td>Sistema turi beveik visus būtinuosius</td><td>„Sistema turi užtikrinti korektišką avarinių saugumo situacijų</td></tr>
</table>

<table>
<tr><th>Kriterijaus pavadinimas</th><th>Kriterijų apibūdinantys klausimai, pvz.,</th><th colspan="3">Vertinimo skalė, parametro apibūdinimas + pavyzdys</th></tr>
<tr><td></td><td></td><td></td><td>atkūrimo mechanizmus, galima išbaigtumo optimizacija</td><td>valdymą, rodyti atitinkamus avarinius pranešimus ir po to savaime grįžti į pradinę darbo būklę“, - nepaaiškinama, iš ko susideda „situacijų valdymas“</td></tr>
<tr><td></td><td></td><td>3</td><td>Sistema turi būtinuosius atkūrimo mechanizmus, bet reikia daugiau išbaigtumo</td><td>„Sistema turi užtikrinti korektišką avarinių saugumo situacijų valdymą, rodyti atitinkamus avarinius pranešimus, sugrįžti į veikimą po kritinių incidentų“, - tik kritiniai atvejai tvarkomi automatiškai</td></tr>
<tr><td></td><td></td><td>2</td><td>Sistemos veikimas atkuriamas, bet ne visais atvejais arba ne visiškai automatiškai</td><td>„Sistema turi rodyti atitinkamus avarinius pranešimus ir po to turi būti sugrąžinama į pradinę darbo būklę“, - bet kai kurios klaidos gali reikalauti rankinio duomenų atkūrimo</td></tr>
<tr><td></td><td></td><td>1</td><td>Yra pavienės atkūrimo reikalavimo dalys, bet jos neapima visų galimų situacijų</td><td>„Sistema turi pristatyti atitinkamus avarinius pranešimus“, - tačiau po neteisingos komandos sistema lieka neveiksni, trūksta informacijos</td></tr>
<tr><td>Duomenų konfidencialumo užtikrinimo aiškumas (K4)</td><td>•Ar duomenų konfidencialumo užtikrinimas yra apibrėžtas vengiant abstrakčių ir neaiškių terminų?
•Ar apibrėžti kontrolės mechanizmai nėra abstraktūs ir pernelyg lakoniški?</td><td>Įvertis</td><td>Aprašymas</td><td>Reikalavimo pvz.,</td></tr>
<tr><td></td><td></td><td>5</td><td>Reikalavimas pakankamai tiksliai apibrėžia kontrolės mechanizmus, nėra vietos interpretacijoms</td><td>„Registro operacinės sistemos lygyje prieiga prie operacinės sistemos resursų ribojama naudojant ACL ir RBAC kontrolės mechanizmus, apsaugant sistemą nuo neteisėto priėjimo prie duomenų bazės failų“</td></tr>
<tr><td></td><td></td><td>4</td><td>Didžioji dalis informacijos aiški, tačiau gali trūkti detalių apie konkrečius įgyvendinimo metodus</td><td>„Registro operacinės sistemos lygyje turi būti kontroliuojamas priėjimas prie operacinės sistemos resursų, prieiga ribojama per prieigos valdymo politiką“, - galėtų būti</td></tr>
</table>

<table>
<tr><th>Kriterijaus pavadinimas</th><th>Kriterijų apibūdinantys klausimai, pvz.,</th><th>Vertinimo skalė, parametro apibūdinimas + pavyzdys</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td></td><td></td><td>papildomai nurodyti konkretūs mechanizmai</td></tr>
<tr><td>3</td><td>Reikalavime nurodytos saugumo priemonės, bet formuluotė vis dar leidžia skirtingas interpretacijas</td><td>„Registro operacinės sistemos lygio saugumas užtikrinamas operacinės sistemos saugumo priemonėmis“, - tačiau vis dar nėra detalizuota, kokios konkrečios priemonės turi būti taikomos</td></tr>
<tr><td>2</td><td>Yra bendra kryptis, bet trūksta tikslumo apie kontrolės mechanizmus</td><td>„Registro operacinės sistemos lygyje turi būti kontroliuojamas priėjimas prie operacinės sistemos resursų“, - tačiau neaišku, kokiomis priemonėmis tai įgyvendinama</td></tr>
<tr><td>1</td><td>Reikalavimas per abstraktus, neapibrėžia, kaip užtikrinamas duomenų konfidencialumas</td><td>„Sistema turi užtikrinti duomenų konfidencialumą“, - tačiau nėra jokios informacijos, kaip tai bus pasiekiama (abstraktu)</td></tr>
</table>
</td></tr>
<tr><td>Atitikties teisinei ir reguliacinei sistemai išsamumas (K5)</td><td>•Ar apibrėžti nacionaliniai (tarptautiniai) teisiniai bei reguliaciniai reikalavimai pakankamai apima aspektus, kuriems yra skirti?</td><td>
<table>
<tr><th>Įvertis</th><th>Aprašymas</th><th>Reikalavimo pvz.,</th></tr>
<tr><td>5</td><td>Reikalavimas pakankamai apima visus teisinius ir reguliacinius aspektus, nurodo standartus bei jų taikymo sritis</td><td>„Registre įgyvendintos saugumo priemonės užtikrina apsaugą nuo OWASP TOP 10, atitinka ISO/IEC 27001, GDPR, NIST 800-53 ir PCI DSS reikalavimus, o jų įgyvendinimas patvirtinamas reguliariais saugumo auditais“.</td></tr>
<tr><td>4</td><td>Apima pagrindinius teisinius ir reguliacinius reikalavimus, bet yra tobulintinas</td><td>„Registre įgyvendintos saugumo priemonės užtikrina apsaugą nuo OWASP TOP 10, atitinka ISO/IEC 27001 ir GDPR reikalavimus dėl duomenų apsaugos“, - bet detalesnė informacija dėl, pvz., sertifikavimo nepateikiama</td></tr>
<tr><td>3</td><td>Nurodytos kelios reguliacinės gairės, bet jos neapima</td><td>„Registre įgyvendintos saugumo priemonės užtikrina apsaugą nuo OWASP TOP 10 ir atitinka bendruosius ISO/IEC 27001</td></tr>
</table>
</td></tr>
</table>

Kriterijaus pavadinimas	*Kriterijų apibūdinantys klausimai, pvz.,*	*Vertinimo skalė, parametro apibūdinimas + pavyzdys*		
			visų aktualių aspektų	reikalavimus“, - **tačiau trūksta išsamumo, kaip tai bus įgyvendinta**
		2	Paminėta viena konkreti saugumo sritis, bet nėra platesnio reguliacinio konteksto	„Registre įgyvendintos saugumo priemonės užtikrina apsaugą nuo OWASP TOP 10“, - **tačiau nėra integracijos su kitomis saugumo praktikomis, pvz., NIST**
		1	Reikalavimas labai ribotas, neapima esminių reguliacinių reikalavimų	„Registre įgyvendintos saugumo priemonės užtikrina apsaugą nuo OWASP TOP 10“, - **tačiau nėra aišku, ar apima ir kitus teisinius ir reguliacinius reikalavimus, pvz., ISO/IEC 27001**

Vertinimo lentelė

Kriterijus / ***Scenarijus***	***K1***	***K2***	***K3***	***K4***	***K5***
1					
2					
3					
4					
5					

1 Scenarijus. Kraujo donorų registro (KDR) normalizuotas techninis aprašas

- *KDR naudotojai turi būti atpažįstami, o jų atliekami veiksmai žymimi naudotojų veiksmų žurnale. Programiniai moduliai turi būti prieinami naudotojams pagal jiems suteiktas teises; funkcionuoti reikalingų paslaugų teikėjo prieiga prie KDR techninės ir programinės įrangos turi būti kontroliuojama naudojant prisijungimo vardų, slaptažodžių ir teisių sistemą, skirtą darbuotojų tapatybei nustatyti;*
- *KDR naudotojai negali turėti galimybės atlikti operacijų tiesiai duomenų bazėje; duomenų bazės lygyje priėjimas prie duomenų turi būti ribojamas teisių ir rolių pagalba. Priėjimui prie duomenų bazių schemų sukurti fiksuoti sisteminiai naudotojai, kuriems leistas tik toks priėjimas kiek reikalauja KDR sistemos naudojimas; duomenų bazės*

administratorius neturės teisės prieiti prie duomenų failų (jei neturės galimybės prieiti prie operacinės sistemos);

- *KDR turi užtikrinti korektišką avarinių saugumo situacijų, kurias sukėlė neteisingi KDR naudotojų veiksmai, neteisingas įvedamų duomenų formatas arba neleidžiamos įvedamų duomenų reikšmės, valdymą. Nurodytais atvejais, atlikus neteisingą (neleidžiamą) komandą arba nekorektiškai įvedus duomenis, KDR turi rodyti atitinkamus avarinius pranešimus ir po to grįžti į pradinę darbo būklę;*
- *KDR operacinės sistemos lygyje turi būti kontroliuojamas priėjimas prie operacinės sistemos resursų, apsaugant sistemą nuo neteisėto priėjimo prie duomenų bazės failų. Operacinės sistemos lygio saugumas užtikrinamas operacinės sistemos saugumo priemonėmis;*
- *KDR įgyvendintos saugumo priemonės užtikrina apsaugą nuo OWASP (angl. „Open Web Application Security Project“) TOP 10 sąraše įvardintų saugumo pažeidimų;*

2 Scenarijus. Mokinių registro (MR) normalizuotas techninis aprašas

- *MR turi būti įgyvendinta galimybė identifikuoti prieigos prie MR duomenų autorius, fiksuoti jų atliktus veiksmus ir juos kaupti; duomenų tvarkytojams prieigos prie duomenų galimybė turi būti tik per registravimosi ir slaptažodžių sistemą;*
- *Prieigos prie MR elektroninės informacijos teises gali suteikti tik MR administratorius. Registro naudotojams suteikiamos tik jų funkcijoms vykdyti būtinos teisės; Visos užklausos į duomenų bazes yra fiksuojamos programiniu būdu, pilnai identifikuojant užklausos autorių ir atliekamą veiksmą;*
- *DBVS turi būti naudojamas LOG failas, kad reikiamu atveju (įvykus avarinei situacijai) pats duomenų bazių serveris atstatytų duomenų bazę iki korektiškos būsenos;*
- *MR naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo; viešaisiais telekomunikaciniais tinklais perduodamos elektroninės informacijos konfidencialumas užtikrinamas naudojant HTTPS (Hypertext Transfer Protocol Secure) protokolą arba šifravimą; užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą iš kitų valstybės institucijų, naudojami saugūs ryšio kanalai, kuriais perduodami šifruoti duomenys;*
- *Būtina sąlyga duomenų apsaugai realizuoti yra norminių aktų, reglamentuojančių duomenų teisinę apsaugą, įgyvendinimas: Lietuvos Respublikos asmens duomenų teisinės*

apsaugos įstatymas; Mokinių registro duomenų saugos nuostatai; Bendrųjų elektroninės informacijos saugos reikalavimų aprašas";

- *Sistema turi būti sukurta vadovaujantis Lietuvos standartais LST ISO/IEC 27001:2013, LST ISO/IEC 27002:2014 ir kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika" grupės standartais; Sąsaja naudotojui turi atitikti W3C standartus ir rekomendacijas;*

3 Scenarijus. Valstybės informacinių technologijų paslaugų valdymo informacinės sistemos (VIPVIS) normalizuotas techninis aprašas

- *Kiekvienas darbuotojas turi asmeninę magnetinę kortelę ir įeidamas į pastatą arba išeidamas iš jo pasižymi įėjimo punktuose; lankytojams ir svečiams privalomai išduodamos svečio elektroninės kortelės. Už apsilankymą atsakingas darbuotojas pasirašo įėjimo punkto žurnale už kiekvieną lankytoją; po 18 val. vakaro ir nedarbo dienomis į pastatą patekti gali tiktai specialius leidimus turintys darbuotojai;*
- *Prisijungti prie kompiuterinio tinklo naudojami VIPVIS naudotojų ID ir prieigos teisių sistema, pagal kurią nustatomos naudotojų teisės tinkle; nuotolinis prisijungimas prie VIPVIS vykdomas protokolu, skirtu duomenims šifruoti; pagal VIPVIS naudotojų atliekamas funkcijas jiems turi būti priskiriami atitinkami prieigos teisių rinkiniai;*
- *VIPVIS administratoriaus naudojamame kompiuteryje turi būti nustatytas VIPVIS naudotojo prieigos blokavimas po tam tikro neaktyvumo laikotarpio, būtina naudoti ekrano apsaugos programą (angl. Screensaver). Neaktyvumo laikotarpis negali būti ilgesnis kaip 15 minučių; saugant vietinį tinklą arba nenaudojamas tinklo jungtis, ribojama fizinė prieiga prie tinklo kabelių, skirstytuvų, atšakų, kartotuvų ir antgalių;*
- *Dingus elektros įtampai sistema automatiškai informuoja atsakingus darbuotojus apie (saugumo) gedimą; esant elektros srovės tiekimo sutrikimų, serverių įrangos veikimas garantuojamas ne mažiau nei 30 minučių ir užtikrinamas saugus programų uždarymas kompiuteriuose, jeigu elektros tiekimas neatsinaujintų;*
- *VIPVIS administratoriaus naudojama kompiuterinė įranga ir elektroninės informacijos laikmenos turi būti laikomos taip, kad pašaliniai asmenys negalėtų prie jų prieiti, paimti ar sugadinti;*
- *VIPVIS naudojamos saugumo priemonės užtikrina apsaugą nuo OWASP (angl. „Open Web Application Security Project") TOP 10 sąraše įvardintų saugumo pažeidimų;*

4 Scenarijus. Žvejybos sektoriaus perleidžiamųjų teisių registro (PTR) normalizuotas techninis aprašas

- *Kiekvienas PTR naudotojas turi būti unikaliai identifikuojamas. Visa identifikavimo informacija turi būti saugoma šifruotu pavidalu tokiu būdu, kad iš saugomos informacijos būtų neįmanoma atkurti pirminių duomenų (pavyzdžiui, slaptažodžių); PTR naudotojas turi patvirtinti savo tapatybę slaptažodžiu arba kitomis nustatytomis identifikavimo ir autentifikavimo patvirtinimo priemonėmis;*
- *PTR turi užtikrinti galimybę nustatyti skirtingus teisių sąrašus pagal PTR naudotojo prisijungimo tipą ir jo tapatybės patikrinimo metodo patikimumą; PTR turi būti prieinamas naudojantis bendromis PTR teikiamomis saugos priemonėmis, bendro prisijungimo (angl. Single Sign On – SSO) principu; Turi būti patvirtinti asmenų, kuriems suteiktos PTR administratoriaus teisės prisijungti prie PTR, sąrašai ir periodiškai peržiūrimi informacijos saugos specialisto. Sąrašas turi būti nedelsiant peržiūrėtas, kai įstatymų nustatytais atvejais PTR administratorius nušalinamas nuo darbo pareigų;*
- *Užtikrinant PTR atkūrimą gedimo atveju turi būti daromos reguliarios rezervinės programos ir duomenų bazės kopijos. Įvykus (saugumo) gedimui, PTR atkūrimo laikas (angl. Recovery Time) turi būti ne ilgesnis kaip 1 darbo diena;*
- *PTR turi palaikyti siunčiamų, gaunamų ir saugomų duomenų užšifravimą ir iššifravimą; Audito duomenys turi būti archyvuojami. Archyve saugomi duomenys turi būti apsaugoti nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo;*
- *Turi būti įgyvendintos LST ISO/IEC 27001:2013 nurodytos techninės saugos priemonės, išskyrus priemones, kurios netaikytinos dėl PTR tvarkytojo veiklos ar PTR naudojamos techninės įrangos pobūdžio. PTR kuriamas vadovaujantis Lietuvos standartais LST ISO/IEC 27001:2013, LST ISO/IEC 27002:2014 ir kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais;*

5 Scenarijus. Nacionalinės turizmo informacinės sistemos (NTIS) normalizuotas techninis aprašas

- *NTIS naudotojui prisijungus prie NTIS naudojant vardų, slaptažodžių ir teisių sistemą, turi būti pateikiama sukonfigūruota naudotojo darbo aplinka ir tik jam prieinami darbui būtini duomenys;*
- *NTIS turi būti atliekamos reguliarios rezervinės programų ir duomenų bazių kopijos; NTIS turi leisti atkurti duomenis iš rezervinių duomenų kopijų;*
- *NTIS turi visapusiškai užtikrinti duomenų konfidencialumą taikydama šifravimą perduodamiems duomenims; pašalinių asmenų priėjimas prie kompiuterinės įrangos ir laikmenų turi būti užkardytas;*

- *NTIS saugumo priemonės turi užtikrinti apsaugą nuo OWASP (angl. Open Web Application Security Project) TOP 10 sąraše įvardintų saugumo pažeidimų;*

5 priedas. Specifikacijų saugumo reikalavimų analizė ir vertinimas (2)

Pateikiama ekspertinės apklausos forma, kurios tikslas – tradiciniu būdu įvertinti skirtingus reikalavimų sąrašus (scenarijus) per jų kokybės prizmę, priskiriant jiems atitinkamas skaitines reikšmes.

Užduotis: nustatyti, eksperto manymu, kiekvieno reikalavimų rinkinio (scenarijaus) saugumo reikalavimų apibrėžties kokybės lygį, atitikimą įvertinant specifine skaitine reikšme.

Eiga: atlikite 2, 3, 4, 5 ir 6 lentelėse pateiktų saugumo reikalavimų rinkinių (scenarijų) apibrėžties kokybės vertinimą 1 lentelėje. Vertinimo skalė apima intervalą nuo 1 iki 5, kur 1 – prasčiausią apibrėžties kokybės lygį nusakantis įvertis, o 5 – geriausią įmanomą saugumo reikalavimų apibrėžties kokybės lygį nusakantis įvertis. Atskiras vertinimo pavyzdys ir instrukcija yra pateikiami dokumento pabaigoje.

Dėmesio! ***Scenarijuose pateikti reikalavimai yra išdėstyti atsitiktine tvarka, o reikalavimo apimamas spektras gali varijuoti!***

Vertinimo lentelė

Scenarijaus Nr.	***Apibrėžties kokybės lygį nusakantis įvertis (1-5)***
1	
2	
3	
4	
5	

1 Scenarijus. Kraujo donorų registro (KDR) normalizuotas techninis aprašas

- *KDR naudotojai turi būti atpažįstami, o jų atliekami veiksmai žymimi naudotojų veiksmų žurnale. Programiniai moduliai turi būti prieinami naudotojams pagal jiems suteiktas teises; funkcionuoti reikalingų paslaugų teikėjo prieiga prie KDR techninės ir programinės įrangos turi būti kontroliuojama naudojant prisijungimo vardų, slaptažodžių ir teisių sistemą, skirtą darbuotojų tapatybei nustatyti;*
- *KDR naudotojai negali turėti galimybės atlikti operacijų tiesiai duomenų bazėje; duomenų bazės lygyje priėjimas prie duomenų turi būti ribojamas teisių ir rolių pagalba. Priėjimui prie duomenų bazių schemų sukurti fiksuoti sisteminiai naudotojai, kuriems leistas tik toks priėjimas kiek reikalauja KDR sistemos naudojimas; duomenų bazės administratorius neturės teisės prieiti prie duomenų failų (jei neturės galimybės prieiti prie operacinės sistemos);*

- *KDR turi užtikrinti korektišką avarinių saugumo situacijų, kurias sukėlė neteisingi KDR naudotojų veiksmai, neteisingas įvedamų duomenų formatas arba neleidžiamos įvedamų duomenų reikšmės, valdymą. Nurodytais atvejais, atlikus neteisingą (neleidžiamą) komandą arba nekorektiškai įvedus duomenis, KDR turi rodyti atitinkamus avarinius pranešimus ir po to grįžti į pradinę darbo būklę;*
- *KDR operacinės sistemos lygyje turi būti kontroliuojamas priėjimas prie operacinės sistemos resursų, apsaugant sistemą nuo neteisėto priėjimo prie duomenų bazės failų. Operacinės sistemos lygio saugumas užtikrinamas operacinės sistemos saugumo priemonėmis;*
- *KDR įgyvendintos saugumo priemonės užtikrina apsaugą nuo OWASP (angl. „Open Web Application Security Project“) TOP 10 sąraše įvardintų saugumo pažeidimų;*

2 Scenarijus. Mokinių registro (MR) normalizuotas techninis aprašas

- *MR turi būti įgyvendinta galimybė identifikuoti prieigos prie MR duomenų autorius, fiksuoti jų atliktus veiksmus ir juos kaupti; duomenų tvarkytojams prieigos prie duomenų galimybė turi būti tik per registravimosi ir slaptažodžių sistemą;*
- *Prieigos prie MR elektroninės informacijos teises gali suteikti tik MR administratorius. Registro naudotojams suteikiamos tik jų funkcijoms vykdyti būtinos teisės; Visos užklausos į duomenų bazes yra fiksuojamos programiniu būdu, pilnai identifikuojant užklausos autorių ir atliekamą veiksmą;*
- *DBVS turi būti naudojamas LOG failas, kad reikiamu atveju (įvykus avarinei situacijai) pats duomenų bazių serveris atstatytų duomenų bazę iki korektiškos būsenos;*
- *MR naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo; viešaisiais telekomunikaciniais tinklais perduodamos elektroninės informacijos konfidencialumas užtikrinamas naudojant HTTPS (Hypertext Transfer Protocol Secure) protokolą arba šifravimą; užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą iš kitų valstybės institucijų, naudojami saugūs ryšio kanalai, kuriais perduodami šifruoti duomenys;*
- *Būtina sąlyga duomenų apsaugai realizuoti yra norminių aktų, reglamentuojančių duomenų teisinę apsaugą, įgyvendinimas: Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas; Mokinių registro duomenų saugos nuostatai; Bendrųjų elektroninės informacijos saugos reikalavimų aprašas“;*

- *Sistema turi būti sukurta vadovaujantis Lietuvos standartais LST ISO/IEC 27001:2013, LST ISO/IEC 27002:2014 ir kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais; Sąsaja naudotojui turi atitikti W3C standartus ir rekomendacijas;*

3 Scenarijus. Valstybės informacinių technologijų paslaugų valdymo informacinės sistemos (VIPVIS) normalizuotas techninis aprašas

- *Kiekvienas darbuotojas turi asmeninę magnetinę kortelę ir įeidamas į pastatą arba išeidamas iš jo pasižymi įėjimo punktuose; lankytojams ir svečiams privalomai išduodamos svečio elektroninės kortelės. Už apsilankymą atsakingas darbuotojas pasirašo įėjimo punkto žurnale už kiekvieną lankytoją; po 18 val. vakaro ir nedarbo dienomis į pastatą patekti gali tiktai specialius leidimus turintys darbuotojai;*
- *Prisijungti prie kompiuterinio tinklo naudojami VIPVIS naudotojų ID ir prieigos teisių sistema, pagal kurią nustatomos naudotojų teisės tinkle; nuotolinis prisijungimas prie VIPVIS vykdomas protokolu, skirtu duomenims šifruoti; pagal VIPVIS naudotojų atliekamas funkcijas jiems turi būti priskiriami atitinkami prieigos teisių rinkiniai;*
- *VIPVIS administratoriaus naudojamame kompiuteryje turi būti nustatytas VIPVIS naudotojo prieigos blokavimas po tam tikro neaktyvumo laikotarpio, būtina naudoti ekrano apsaugos programą (angl. Screensaver). Neaktyvumo laikotarpis negali būti ilgesnis kaip 15 minučių; saugant vietinį tinklą arba nenaudojamas tinklo jungtis, ribojama fizinė prieiga prie tinklo kabelių, skirstytuvų, atšakų, kartotuvų ir antgalių;*
- *Dingus elektros įtampai sistema automatiškai informuoja atsakingus darbuotojus apie (saugumo) gedimą; esant elektros srovės tiekimo sutrikimų, serverių įrangos veikimas garantuojamas ne mažiau nei 30 minučių ir užtikrinamas saugus programų uždarymas kompiuteriuose, jeigu elektros tiekimas neatsinaujintų;*
- *VIPVIS administratoriaus naudojama kompiuterinė įranga ir elektroninės informacijos laikmenos turi būti laikomos taip, kad pašaliniai asmenys negalėtų prie jų prieiti, paimti ar sugadinti;*
- *VIPVIS naudojamos saugumo priemonės užtikrina apsaugą nuo OWASP (angl. „Open Web Application Security Project“) TOP 10 sąraše įvardintų saugumo pažeidimų;*

4 Scenarijus. Žvejybos sektoriaus perleidžiamųjų teisių registro (PTR) normalizuotas techninis aprašas

- *Kiekvienas PTR naudotojas turi būti unikaliai identifikuojamas. Visa identifikavimo informacija turi būti saugoma šifruotu pavidalu tokiu būdu, kad iš saugomos*

informacijos būtų neįmanoma atkurti pirminių duomenų (pavyzdžiui, slaptažodžių); PTR naudotojas turi patvirtinti savo tapatybę slaptažodžiu arba kitomis nustatytomis identifikavimo ir autentifikavimo patvirtinimo priemonėmis;

- *PTR turi užtikrinti galimybę nustatyti skirtingus teisių sąrašus pagal PTR naudotojo prisijungimo tipą ir jo tapatybės patikrinimo metodo patikimumą; PTR turi būti prieinamas naudojantis bendromis PTR teikiamomis saugos priemonėmis, bendro prisijungimo (angl. Single Sign On – SSO) principu; Turi būti patvirtinti asmenų, kuriems suteiktos PTR administratoriaus teisės prisijungti prie PTR, sąrašai ir periodiškai peržiūrimi informacijos saugos specialisto. Sąrašas turi būti nedelsiant peržiūrėtas, kai įstatymų nustatytais atvejais PTR administratorius nušalinamas nuo darbo pareigų;*
- *Užtikrinant PTR atkūrimą gedimo atveju turi būti daromos reguliarios rezervinės programos ir duomenų bazės kopijos. Įvykus (saugumo) gedimui, PTR atkūrimo laikas (angl. Recovery Time) turi būti ne ilgesnis kaip 1 darbo diena;*
- *PTR turi palaikyti siunčiamų, gaunamų ir saugomų duomenų užšifravimą ir iššifravimą; Audito duomenys turi būti archyvuojami. Archyve saugomi duomenys turi būti apsaugoti nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo;*
- *Turi būti įgyvendintos LST ISO/IEC 27001:2013 nurodytos techninės saugos priemonės, išskyrus priemones, kurios netaikytinos dėl PTR tvarkytojo veiklos ar PTR naudojamos techninės įrangos pobūdžio. PTR kuriamas vadovaujantis Lietuvos standartais LST ISO/IEC 27001:2013, LST ISO/IEC 27002:2014 ir kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais;*

5 Scenarijus. Nacionalinės turizmo informacinės sistemos (NTIS) normalizuotas techninis aprašas

- *NTIS naudotojui prisijungus prie NTIS naudojant vardų, slaptažodžių ir teisių sistemą, turi būti pateikiama sukonfigūruota naudotojo darbo aplinka ir tik jam prieinami darbui būtini duomenys;*
- *NTIS turi būti atliekamos reguliarios rezervinės programų ir duomenų bazių kopijos; NTIS turi leisti atkurti duomenis iš rezervinių duomenų kopijų;*
- *NTIS turi visapusiškai užtikrinti duomenų konfidencialumą taikydama šifravimą perduodamiems duomenims; pašalinių asmenų priėjimas prie kompiuterinės įrangos ir laikmenų turi būti užkardytas;*
- *NTIS saugumo priemonės turi užtikrinti apsaugą nuo OWASP (angl. Open Web Application Security Project) TOP 10 sąraše įvardintų saugumo pažeidimų;*

6 priedas. Ekspertų E1, E7, E6 ir E2 saugumo reikalavimų rinkinių vertinimo suvestinės skaitinėmis (kiekybinėmis) reikšmėmis

E1 eksperto saugumo reikalavimų rinkinių vertinimo suvestinė skaitinėmis reikšmėmis

Kriterijus / *Scenarijus*	***K1***	***K2***	***K3***	***K4***	***K5***
1	3	4	3	3	1
2	2	4	4	2	3
3	4	3	3	4	4
4	5	3	4	5	5
5	3	2	3	2	3

E7 eksperto saugumo reikalavimų rinkinių vertinimo suvestinė skaitinėmis reikšmėmis

Kriterijus / *Scenarijus*	***K1***	***K2***	***K3***	***K4***	***K5***
1	4	5	3	3	2
2	3	4	2	3	3
3	5	5	4	4	3
4	5	5	4	5	5
5	3	3	2	3	3

E6 eksperto saugumo reikalavimų rinkinių vertinimo suvestinė skaitinėmis reikšmėmis

Kriterijus / *Scenarijus*	***K1***	***K2***	***K3***	***K4***	***K5***
1	4	3	4	5	4
2	3	3	4	4	4
3	5	4	4	5	4
4	3	2	3	3	3
5	3	3	3	2	2

E2 eksperto saugumo reikalavimų rinkinių vertinimo suvestinė skaitinėmis reikšmėmis

Kriterijus / *Scenarijus*	***K1***	***K2***	***K3***	***K4***	***K5***
1	4	5	3	4	4
2	5	4	4	4	5
3	3	5	5	3	5
4	3	4	5	4	5

Kriterijus / *Scenarijus*	*K1*	*K2*	*K3*	*K4*	*K5*
5	2	3	3	3	2

7 priedas. Ekspertų E1, E7, E6 ir E2 saugumo reikalavimų rinkinių vertinimo suvestinės lingvistinėmis (kokybinėmis) reikšmėmis

E1 eksperto saugumo reikalavimų rinkinių vertinimo suvestinė lingvistinėmis reikšmėmis

Kriterijus / *Scenarijus*	***K1***	***K2***	***K3***	***K4***	***K5***
1	V	A	V	V	LŽ
2	Ž	A	A	Ž	V
3	A	V	V	A	A
4	LA	V	A	LA	LA
5	V	Ž	V	Ž	V

E7 eksperto saugumo reikalavimų rinkinių vertinimo suvestinė lingvistinėmis reikšmėmis

Kriterijus / *Scenarijus*	***K1***	***K2***	***K3***	***K4***	***K5***
1	A	LA	V	V	Ž
2	V	A	Ž	V	V
3	LA	LA	A	A	V
4	LA	LA	A	LA	LA
5	V	V	Ž	V	V

E6 eksperto saugumo reikalavimų rinkinių vertinimo suvestinė lingvistinėmis reikšmėmis

Kriterijus / *Scenarijus*	***K1***	***K2***	***K3***	***K4***	***K5***
1	A	V	A	LA	A
2	V	V	A	A	A
3	LA	A	A	LA	A
4	V	Ž	V	V	V
5	V	V	V	Ž	Ž

E2 eksperto saugumo reikalavimų rinkinių vertinimo suvestinė lingvistinėmis reikšmėmis

Kriterijus / *Scenarijus*	***K1***	***K2***	***K3***	***K4***	***K5***
1	A	LA	V	A	A
2	LA	A	A	A	LA
3	V	LA	LA	V	LA
4	V	A	LA	A	LA

Kriterijus / *Scenarijus*	*K1*	*K2*	*K3*	*K4*	*K5*
5	Ž	V	V	V	Ž

8 priedas. Lietuvos jaunųjų mokslininkų konferencijos (JMK) „Mokslas – Lietuvos ateitis“ dalyvio pažymėjimas

VILNIUS TECH
Fundamentinių mokslų fakultetas

PAŽYMĖJIMAS

Nr. 25-0416-23

Rytis Šakalys

2025 m. balandžio 16 d. dalyvavo
28-osios Lietuvos jaunųjų mokslininkų konferencijos
„Mokslas – Lietuvos ateitis“ teminėje konferencijoje
Informacinių technologijų sauga ir informacinės sistemos.
Sesijoje „Informacinių technologijų sauga“ pristatė pranešimą
„Daugiakriterių metodų taikymas registrų ir informacinių sistemų specifikacijų saugumo reikalavimų kokybei vertinti“.

Mokslo komiteto pirmininkas prof. dr. Nikolaj Goranin

Organizacinio komiteto pirmininkas prof. dr. Diana Kalibatienė

Vilnius, 2025