VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

FUNDAMENTINIŲ MOKSLŲ FAKULTETAS

INFORMACINIŲ SISTEMŲ KATEDRA

Simas Balevičius

DAUGIAKRITERIŲ METODŲ TAIKYMAS INFORMACIJOS SAUGOS METRIKOMS TOBULINTI

APPLICATION OF MULTICRITERIA METHODS FOR IMPROVEMENT OF INFORMATION SECURITY METRICS

Baigiamasis magistro darbas

Informacijos ir informacinių technologijų saugos studijų programa, valstybinis kodas 6211BX014

Informatikos inžinerijos studijų kryptis

Vadovas doc. dr. Nikolaj Goranin

Vilnius, 2022

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

FUNDAMENTINIŲ MOKSLŲ FAKULTETAS

INFORMACINIŲ SISTEMŲ KATEDRA

TVIRTINU
Katedros vedėjas

_____
(Parašas)
doc. dr. Nikolaj Goranin
(Vardas, pavardė)

_____
(Data)

Simas Balevičius

DAUGIAKRITERIŲ METODŲ TAIKYMAS INFORMACIJOS SAUGOS METRIKOMS TOBULINTI

APPLICATION OF MULTICRITERIA METHODS FOR IMPROVEMENT OF INFORMATION SECURITY METRICS

Baigiamasis magistro darbas

Informacijos ir informacinių technologijų saugos studijų programa, valstybinis kodas 6211BX014

Informatikos inžinerijos studijų kryptis

Vadovas doc. dr. Nikolaj Goranin _____ _____
(Moksl. laipsnis, vardas, pavardė) (Parašas) (Data)

Lietuvių kalbos konsultantas dr. Vaida Buivydienė _____ _____
(Moksl. laipsnis, vardas, pavardė) (Parašas) (Data)

Vilnius, 2022

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
FUNDAMENTINIŲ MOKSLŲ FAKULTETAS
INFORMACINIŲ SISTEMŲ KATEDRA

TVIRTINU
Katedros vedėjas

_____
(Parašas)
doc. dr. Nikolaj Goranin
(Vardas, pavardė)

_____
(Data)

Informatikos inžinerijos studijų kryptis

Informacijos ir informacinių technologijų studijų programa, valstybinis kodas 6211BX014

BAIGIAMOJO MAGISTRO DARBO
UŽDUOTIS

..... Nr. .....
Vilnius

Studentui Simui Balevičiui
(Vardas, pavardė)

Baigiamojo darbo tema: Daugiakriterių metodų taikymas informacijos saugos metrikoms tobulinti

patvirtinta 2020 m lapkričio 11 d. dekano potvarkiu Nr. 329fm

Baigiamojo darbo užbaigimo terminas 2022 m. ..... d.

BAIGIAMOJO DARBO UŽDUOTIS:

Darbo tikslas yra įvertinti daugiakriterių metodų pritaikomumą informacijos saugos metrikoms tobulinti. Uždaviniai: 1) Atlikti egzistuojančių metrikų analizę bei daugiakriterių metodų panaudojimą informacijos saugos valdymo srityje; 2) Pasiūlyti daugiakriterį vertinimo būdą; 3) Eksperimentiškai įgyvendinti metodą ir įvertinti gautus rezultatus.

Baigiamojo darbo rengimo konsultantai:

.....

.....
(Moksl. laipsnis/pedag. vardas, vardas, pavardė)

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

Užduotį gavau

.....
(Parašas)

Simas Balevičius
(Vardas, pavardė)

2020-10-13
(Data)

Vilniaus Gedimino technikos universitetas

Fundamentinių mokslų fakultetas

Informacinių sistemų katedra

ISBN ISSN

Egz. sk. .....

Data .....-.....-.....

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

Daugiakriterių metodų taikymas informacijos saugos metrikoms tobulinti

Autorius **Simas Balevičius**

Vadovas **Nikolaj Goranin**

Kalba: lietuvių

Anotacija

Darbe aprašomas daugiakriterių sprendimo priėmimo metodų taikymas siekiant tobulinti informacijos saugos metrikas. Tobulinimas atliekamas pasiūlant agreguotas metrikas. Jos gaunamos ekspertinio vertinimo būdu ir yra siūlomos trims ISO/IEC 27001 informacijos saugos standarto valdymo sritims. Pirmuoju tyrimo etapu atrenkamos tinkamiausios įvairiuose šaltiniuose minimos klasikinės informacijos saugos metrikos. Vėliau taikomi du problemos sprendimo būdai, apimantys daugiakriterius metodus: AHP, WASPAS ir „Fuzzy“ TOPSIS. Siūlomos trys agreguotos informacijos saugos metrikos, kuriose vertinama kiekvienos atrinktos klasikinės metrikos svarba, suteikiant svorio koeficientus. Gautų agreguotų metrikų taikymo pranašumai ir trūkumai aprašomi verifikavimo eksperimento dalyje.

Darbą sudaro 7 dalys: įvadas, analitinė dalis, eksperimento eigos aprašymas, eksperimento vykdymas, verifikavimo eksperimentas, išvados, literatūra. Darbo apimtis: 67 p. teksto be priedų, 9 iliustracijos., 35 lent., 53 bibliografiniai šaltiniai. Atskirai pridedami darbo priedai.

Prasminiai žodžiai: Informacijos saugos metrikos, daugiakriteriai sprendimų priėmimo metodai, agreguotos informacijos saugos metrikos, 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 Multicriteria Methods for Improvement of Information Security Metrics**

Author **Simas Balevičius**

Academic supervisor **Nikolaj Goranin**

Thesis language: Lithuanian

Annotation

The paper describes an application of multi-criteria decision-making methods for the improvement of information security metrics. The improvement is done by proposing aggregated metrics. These are derived from expert judgment and are proposed for the three management domains of the ISO/IEC 27001 information security standard. In the first phase of the study, the selection of the most relevant classical information security metrics that are being mentioned in various sources is performed. Later, two approaches to the problem are applied, involving multi-criteria methods: AHP, WASPAS and Fuzzy TOPSIS. Three aggregated information security metrics are proposed, in which the importance of each selected classical metric is evaluated by giving weighting factors. The advantages and disadvantages of applying the resulting aggregated metrics are described in the verification experiment section.

The work consists of 7 parts: introduction, analytical part, description of the experimental procedure, execution of the experiment, verification experiment, conclusions, and references. Scope of work: 67 pages of text without appendices, 9 illustrations, 35 tables, and 53 references. Annexes to the thesis are attached separately.

Keywords: Information security metrics, multi-criteria decision making methods, aggregated information security metrics, AHP, WASPAS, Fuzzy TOPSIS.

Vilniaus Gedimino technikos universiteto egzaminų sesijų ir baigiamųjų darbų rengimo bei gynimo organizavimo tvarkos aprašo
2 priedas

(Baigiamojo darbo sąžiningumo deklaracijos forma)

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Simas Balevičius, 20162232

(Studento vardas ir pavardė, studento pažymėjimo Nr.)

Fundamentinių mokslų fakultetas

(Fakultetas)

Informacijos ir informacinių technologijų sauga, ITSfm-20

(Studijų programa, akademinė grupė)

BAIGIAMOJO DARBO (PROJEKTO) SĄŽININGUMO DEKLARACIJA

2022 m. gegužės 20 d.

Patvirtinu, kad mano baigiamasis darbas tema „Daugiakriterių metodų taikymas informacijos saugos metrikoms tobulinti“ patvirtintas 2020 m. lapkričio 11 d. dekano potvarkiu Nr. 329fm, yra savarankiškai parašytas. Šiame darbe pateikta medžiaga nėra plagijuota. Tiesiogiai ar netiesiogiai panaudotos kitų šaltinių citatos pažymėtos literatūros nuorodose.

Mano darbo vadovas docentas daktaras Nikolaj Goranin.

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

(Parašas) Simas Balevičius

(Vardas ir pavardė)

Turinys

Iliustracijų sąrašas 8
Lentelių sąrašas 8
Santrumpos ir terminų žodynas 10
1. Įvadas 11
2. Informacijos saugos metrikų tobulinimo ir MCDM metodų panaudojimo apžvalga 14
2.1. Informacijos saugos metrikos 14
2.1.1. Informacijos saugos metrikų samprata ir kokybės kriterijai 14
2.1.2. Informacijos saugos metrikų tipai ir pavyzdžiai 18
2.1.3. Agreguotos informacijos saugos metrikos 23
2.2. Daugiakriteriai sprendimų priėmimo metodai 24
2.2.1. Daugiakriterių sprendimų priėmimo metodų samprata ir klasifikacija 24
2.2.2. Daugiakriterių sprendimų priėmimo metodų palyginimas 24
2.3. Moksliniuose darbuose naudojami informacijos saugos metrikų vertinimo, optimizavimo ir tobulinimo metodai 28
2.4. Apžvalgos apibendrinimas, išvados ir tolimesni darbai 29
3. Agreguotų informacijos saugos metrikų sudarymo eigos aprašymas 31
3.1. Agreguotų informacijos saugos metrikų apibūdinimas 31
3.2. Klasikinės informacijos saugos metrikos, skirtos agreguotoms metrikoms sudaryti 33
3.3. MCDM metodų taikymas agreguotai informacijos saugos metrikai sudaryti 38
3.3.1. MCDM taikymo aprašymas 38
3.3.2. AHP taikymas kriterijų svorių nustatymui 40
3.3.3. WASPAS taikymo, agreguotai informacijos saugos metrikai sudaryti, aprašymas 43
3.3.4. Fuzzy TOPSIS taikymo, agreguotai informacijos saugos metrikai sudaryti, aprašymas 45
4. MCDM taikymas ir ekspertinis vertinimas agreguotoms informacijos saugos metrikoms sudaryti 48
4.1. Ekspertų grupė 48
4.2. Agreguotų metrikų sudarymas 48
4.3. Ekspertų nuomonių suderinamumo patikrinimas 57
5. Verifikavimo eksperimentas 60
6. Išvados 62
7. Literatūra 63
Priedai 67

Iliustracijų sąrašas

1 pav. Agreguotų metrikų sudarymas taikant MCDM. Uždavinio hierarchinė struktūra

2 pav. Užduoties sprendimo metodika

3 pav. Operacijų saugos klasikinių metrikų svorio koeficientai agreguotoje metrikoje gauti skirtingais problemos sprendimo būdais

4 pav. Komunikacijų saugos klasikinių metrikų svorio koeficientai agreguotoje metrikoje gauti skirtingais problemos sprendimo būdais

5 pav. Informacinių sistemų įsigijimo, tobulinimo ir priežiūros saugos klasikinių metrikų svorio koeficientai agreguotoje metrikoje gauti skirtingais problemos sprendimo būdais

6 pav. Kendall‘o W konkordancijos koeficientai apskaičiuoti skirtingoms ekspertinio vertinimo sritims

7 pav. Pradiniai verifikavimo eksperimento duomenys skirti ataskaitos ruošimui (klasikinių metrikų duomenys)

8 pav. Pradiniai verifikavimo eksperimento duomenys skirti ataskaitos ruošimui (agreguotų metrikų duomenys)

9 pav. Agreguotų ir klasikinių metrikų taikymo palyginimo rezultatai

Lentelių sąrašas

1 lentelė. Moksliniuose darbuose naudojami informacijos saugos metrikų apibrėžimai (Yasasin & Schryen, 2015)

2 lentelė. Literatūroje išskiriami pagrindiniai informacijos saugos metrikų kokybės kriterijai (Yasasin & Schryen, 2015)

3 lentelė. Informacijos saugos metrikų lentelė. Perimetro apsauga (Jaquith, 2007)

4 lentelė. Informacijos saugos metrikų lentelė. Apimties ir valdymo sritis (Jaquith, 2007)

5 lentelė. Informacijos saugos metrikų lentelė. Informacijos pasiekiamumas ir sistemų patikimumas (Jaquith, 2007)

6 lentelė. Daugiakriterių metodų palyginimas (Poškas et al., 2012)

7 lentelė. MCDM metodų apibendrinimas (Siksnelyte-Butkiene et al., 2020; Velasquez & Hester, 2013)

8 lentelė. Agreguotos informacijos saugos metrikos pavyzdžio parametrai

9 lentelė. Agreguotos informacijos saugos metrikos formulės verčių apibūdinimas

10 lentelė. Operacijų saugos srities klasikinės informacijos saugos metrikos, kurios bus naudojamos agreguotos metrikos sudarymui (Fasulo, 2019; Jaquith, 2007; Zhang, 2017)

11 lentelė. Komunikacijų saugos srities klasikinės informacijos saugos metrikos, kurios bus naudojamos agreguotos metrikos sudarymui (Fasulo, 2019; Jaquith, 2007; Zhang, 2017)

12 lentelė. Informacinių sistemų įsigijimo, tobulinimo ir priežiūros srities klasikinės informacijos saugos metrikos, kurios bus naudojamos agreguotos metrikos sudarymui (Fasulo, 2019; Jaquith, 2007; Zhang, 2017)

13 lentelė. Klasikinių informacijos saugos metrikų reitingavimo sprendimų matrica

14 lentelė. Porinio palyginimo matrica

15 lentelė. Kokybinių, metriką apibūdinančių, kriterijų porinio palyginimo matrica (Poškas et al., 2012)

16 lentelė. AHP metodo kokybinių kriterijų porinio palyginimo skalė (Poškas et al., 2012; Saaty, 1987)

17 lentelė. Ekspertų lingvistinių apibūdinimų konvertavimas į skaitines vertes (Badalpur & Nurbakhsh, 2019)

18 lentelė. Lingvistinių verčių konvertavimas į skaitines taikant Fuzzy TOPSIS metodą (reitingams) (Chen, 2000)

19 lentelė. Atsakymai į klausimyno klausimus (klasikinių informacijos saugos metrikų pasirinkimai)

20 lentelė. Klasikinių saugos metrikų simboliniai žymėjimai

21 lentelė. AHP metodas. Ekspertų pateikti metrikos kokybės poriniai kriterijų vertinimai (kur, E – ekspertas nr. X, K – korektiškumas, G – galimybė išmatuoti, R – reikšmingumas, A – apibendrintas vertinimas)

22 lentelė. Fuzzy TOPSIS metodas. Ekspertų pateikti kokybės kriterijų vertinimai (kur, E – ekspertas nr. X, K – korektiškumas, G – galimybė išmatuoti, R – reikšmingumas)

23 lentelė. Sprendimų priėmimo matricos (WASPAS)

24 lentelė. Normalizuotos sprendimų priėmimo matricos (WASPAS)

25 lentelė. Pirmojo optimalumo kriterijaus vertės (WASPAS)

26 lentelė. Antrojo optimalumo kriterijaus vertės (WASPAS)

27 lentelė. Bendrojo optimalumo kriterijaus vertės ir klasikinių metrikų svoriai agreguotoje metrikoje (WASPAS)

28 lentelė. Sprendimų priėmimo matrica (Fuzzy TOPSIS)

29 lentelė. Normalizuotos sprendimų priėmimo matricos (Fuzzy TOPSIS)

30 lentelė. Svertinės normalizuotos sprendimų priėmimo matricos (Fuzzy TOPSIS)

31 lentelė. Teigiamai idealios (FPIS, A+) ir neigiamai idealios (FNIS, A-) alternatyvų vertės (Fuzzy TOPSIS)

32 lentelė. Santykiniai atstumai, atstumai iki idealios alternatyvos ir klasikinių metrikų svoriai agreguotoje metrikoje (Fuzzy TOPSIS)

33 lentelė. Skirtingais problemos sprendimo būdais gautos klasikinių metrikų vertės agreguotoje metrikoje

34 lentelė. Ekspertinio vertinimo suderinamumo skaičiavimai

35 lentelė. Ekspertų atsakymai į verifikavimo eksperimento klausimyną

Santrumpos ir terminų žodynas

AHP (angl. *analytic hierarchy process*) – analitinis hierarchijos procesas

CIA triada (angl. *CIA triad*) – konfidencialumo, integralumo ir prieinamumo triada

CISO (angl. *chief executive security officer*) – vyriausiasis informacijos saugos vadovas

CIO (angl. *chief information officer*) – vyriausiasis informacijos vadovas

Fuzzy – neapibrėžtumas

Fuzzy TOPSIS (angl. *technique for order preference by similarity to ideal solution*) – neapibrėžtasis eiliškumo pagal panašumą į idealų sprendimą metodas

IDS (angl. *intrusion detection system*) – įsilaužimo aptikimo sistema

KPI (angl. *key performance indicator*) – pagrindinis veiklos rodiklis

KPK – kenksmingas programinis kodas

MCDM/MCDA (angl. *multiple-criteria decision making/analysis*) – daugiakriteris sprendimų priėmimas/analizė

MTBF (angl. *mean time between failures*) – vidutinis laikas tarp gedimų

MTTR (angl. *mean time to repair*) – vidutinis gedimo šalinimo laikas

OS – operacinė sistema

SIEM (angl. *security information and event management*) – saugumo informacijos ir įvykių valdymas

TOPSIS (angl. *technique for order preference by similarity to ideal solution*) – eiliškumo pagal panašumą į idealų sprendimą metodas

WASPAS (angl. *weighted aggregated sum product assessment*) – svertinės agreguotos sumos daugybos metodas

WSM (angl. *weighted sum method*) – svertinės sumos metodas

WPM (angl. *weighted product method*) – svertinės daugybos metodas

1. Įvadas

Informacijos sauga apima organizacijos lėšų apsaugą, įmonės funkcijų nenutrūkstamumo, duomenų bei jautrios informacijos integralumo ir privatumo išlaikymą (Caballero, 2014). Aiškinant informacijos saugos tikslus, mokslinėje literatūroje dažniausiai minima CIA triados sąvoka. CIA triadoje apibrėžiama, kad informacijos saugos užduotis yra užtikrinti, informacijos konfidencialumą, integralumą ir prieinamumą. (Qadir & Quadri, 2016).

Didžioji dalis pasaulyje veikiančių organizacijų negali veikti be informacijos saugos priemonių. Dirbant tam tikrose srityse, pavyzdžiui, finansų sektoriuje, reikalaujama laikytis įvairių standartų ir reikalavimų, susijusių su informacijos sauga. Ne išimtis ir kompanijos iš kitų sričių, tokių kaip: energetika, medicina, logistika, krašto apsauga ir t. t.

Siekdamos užtikrinti informacijos saugą, organizacijos yra priverstos tam skirti resursus. Resursų planavimu ir išnaudojimu, dažniausiai rūpinasi informacijos saugos vadovas – CISO. CISO sudaro saugumo programą ir yra atsakingas už jos taikymą. Norint įsitikinti taikomos programos efektyvumu, reikia atlikti matavimus. Būtent šie matavimai yra vadinami informacijos saugos metrikomis. Metrikos leidžia įvertinti saugumo situaciją bei ilgainiui suprasti taikomos informacijos saugos programos efektyvumą. Metrikų taikymas yra apibrėžiamas ir tarptautiniame informacijos saugos valdymo standarte ISO/IEC 27004 (ISO/IEC, 2016).

Baigiamajame darbe aprašomas daugiakriterių sprendimų priėmimo metodų (MCDM) pritaikymas, informacijos saugos metrikų tobulinimui atlikti. Siekiama įvertinti šiuo metu naudojamas klasikines informacijos saugos metrikas ir pasiūlyti naujas – agreguotas metrikas.

Agreguotos metrikos pateikia apibendrintą požiūrį į organizacijos informacijos saugos padėtį. Jų taikymas leidžia efektyviau suprasti esamą saugos situaciją, taip pat gali leisti sumažinti stebėjimui skiriamus resursus.

Tyrimo objektas – informacijos saugos metrikos ir daugiakriteriai sprendimų priėmimo metodai.

Darbo tikslas – taikant daugiakriterius sprendimų priėmimo metodus (MCDM), atlikti informacijos saugos metrikų tobulinimą. Tai bus pasiekta pasiūlant agreguotas informacijos saugos metrikas ir įvertinant jų taikymo efektyvumą.

Uždaviniai:

1. Išanalizuoti egzistuojantį saugumo metrikų bei daugiakriterių sprendimo priėmimo metodų panaudojimą informacijos saugos valdymo srityje.

2. Pasiūlyti metodiką, kuri leistų gauti agreguotas informacijos saugos metrikas pritaikant daugiakriterius sprendimų priėmimų metodus.
3. Gauti agreguotas metrikas (sudarytas iš dabar naudojamų klasikinių informacijos saugos metrikų), kurios atskleistų apibendrintą požiūrį į organizacijos informacijos saugos padėtį.
4. Atlikti verifikavimo eksperimentą, kuriame būtų lyginami klasikinių ir agreguotų informacijos saugos metrikų taikymo privalumai ir trūkumai.

Temos naujumas bei praktinė vertė:

Elektroninėje erdvėje nuolatos vyksta nusikaltimai nukreipti prieš organizacijas. Tai skatina informacijos saugos specialistus dirbti bei vykdyti saugumo programas. Šių programų efektyvumą priimta matuoti metrikomis. Metrikos yra itin svarbios, kadangi jos teikia tiesioginę informaciją apie organizacijos informacijos saugos padėtį. Efektyvus metrikų panaudojimas gali išspręsti organizacijų saugumo problemas. Tai atitinkamai leistų sumažinti nusikaltimų elektroninėje erdvėje skaičių. Darbu siekiama tobulinti metrikas, o tai iš esmės gali stipriai prisidėti prie organizacijos saugumo padėties gerinimo. Tema nauja ir aktuali, kadangi informacijos saugos metrikų taikymas dar nėra organizacijose galutinai nusistovėjęs procesas. Mokslo bendruomenei yra būtina šiuo metu taikomas metrikas susisteminti, išrinkti geriausias, patobulinti esamas ar pasiūlyti naujas – agreguotas. Agreguotų metrikų sudarymui darbe bus naudojami daugiakriteriai sprendimų priėmimo metodai.

Tyrimo metodika:

1. Analitinei daliai atlikti buvo naudojama su tema susijusių mokslinių straipsnių literatūros analizė.
2. Tyrimo metodikos dalyje pristatomos agreguotos informacijos saugos metrikos sąvoka.
3. Trims ISO/IEC 27001 informacijos saugos valdymo standarto sritims siūlomos dažniausiai mokslinėje literatūroje ir praktikoje pasitaikančios klasikinės informacijos saugos metrikos.
4. Ekspertinio vertinimo būdu, skirtingoms informacijos saugos valdymo sritims atrenkamos geriausios klasikinės saugos metrikos iš pasiūlytų metrikų sąrašo.
5. Naudojantis daugiakriteriais sprendimų priėmimo metodais, iš atrinktų klasikinių saugos metrikų, sudaromos agreguotos informacijos saugos metrikos, kurios teikia apibendrintą požiūrį į organizacijos informacijos saugos padėtį.
6. Atliekamas darbe gautų agreguotų informacijos saugos metrikų efektyvumo tyrimas.

Mokslinė darbo vertė – mokslinis darbas prisidės prie kitų tyrimų atliekamų informacijos saugos metrikų srityje. Informacijos saugos sektorius yra vienas iš tų vadybinių sektorių, kuris neturi itin aiškių ir tvirtai nusistovėjusių metodikų, kaip vertinti su sauga vykstančius procesus kiekybiškai (Jaquith, 2007). Matavimus susijusius su informacijos saugos valdymo procesais apibrėžia ISO/IEC 27004 standartas

(ISO/IEC, 2016). Tačiau metrikų taikymas organizacijose yra pakankamai individualus ir nuo daugelio veiksnių priklausantis procesas. Darbe siūloma tobulinti klasikines informacijos saugos metrikas jas sujungiant į bendrą – agreguotą metriką. Siūloma metodika, kaip šį procesą galima būtų įgyvendinti taikant MCDM.

Mokslinis darbas turėtų prisidėti prie informacijos saugos metrikų vystymo. Tobulesnės, metrikos turėtų prisidėti prie organizacijų informacijos saugos tobulinimo. Agreguota metrika turėtų leistų efektyviau įvertinti informacijos saugos padėtį organizacijoje.

Darbo rezultatai:

1. Atlikta literatūros šaltinių, susijusių su informacijos saugos metrikomis ir daugiakriteriais sprendimų priėmimo metodais, analizė.
2. Aprašyta daugiakriterių sprendimo priėmimo metodų panaudojimo metodologija, skirta agreguotoms informacijos saugos metrikoms gauti.
3. Trims ISO/IEC 27001 standarto valdymo sritims pasiūlytos agreguotos informacijos saugos metrikos.
4. Verifikavimo eksperimento dalyje įvertinamas agreguotų metrikų naudojimas, jas lyginant su klasikinėmis metrikomis.

Darbo struktūra:

1. Darbą sudaro 7 skyriai, tai įvadas, analitinė dalis (informacijos saugos metrikų ir MCDM metodų panaudojimo apžvalga), siūlomas agreguotų informacijos saugos metrikų sudarymo aprašymas, MCDM taikymas agreguotoms metrikoms sudaryti, verifikavimo eksperimentas, išvados ir literatūros sąrašas.
2. Analitinę dalį sudaro 3 skyriai, kuriuose aptariamos egzistuojančios informacijos saugos metrikos, daugiakriteriai sprendimų priėmimo metodai. Taip pat aptariami moksliniai tyrimai, kurių pagrindinis tikslas įvertinti, optimizuoti ir tobulinti informacijos saugos metrikas, taikant įvairaus tipo priemones.
3. Siūlomas informacijos saugos metrikų įvertinimo ir naujų daugiakriterių, agreguotų, metrikų sudarymo metodas susideda iš 3 skyrių: agreguotų informacijos saugos metrikų apibūdinimo, klasikinių informacijos saugos metrikų, skirtų agreguotų metrikų sudarymui, ir daugiakriterių sprendimo priėmimo metodų (MCDM) taikymo agreguotai informacijos saugos metrikai sudaryti aprašymo.
4. MCDM taikymo skyriuje aprašoma tiksli atlikto eksperimento eiga, pateikiami ekspertinio vertinimo rezultatai ir atlikti skaičiavimai.

2. Informacijos saugos metrikų tobulinimo ir MCDM metodų panaudojimo apžvalga

Analitinėje dalyje apibrėžiama informacijos saugos metrikų sąvoka, apibendrinamas požiūris, kodėl yra reikalinga ir naudinga su informacijos sauga susijusius procesus nagrinėti pasitelkiant skaičius (kiekybiškai). Pateikiamas saugos metrikų klasifikavimas ir metrikų pavyzdžiai. Aptariamos galimos daugiakriterės sprendimo priėmimo metodikos (MCDM). Nagrinėjama mokslinė literatūra, susijusi su daugiakriterių metodų taikymu informacijos saugos valdymo srityje bei metrikų vertinimu, optimizavimu ir tobulinimu.

2.1. Informacijos saugos metrikos

Šiame skyriuje bus kalbama apie informacijos saugos metrikų sampratą. Apie tai kokią naudą gauname, atlikdami su informacijos sauga susijusių procesų stebėjimą taikant skaičius (šiuos procesus tiriant kiekybiškai). Organizacijos veikloje yra labai svarbu turėti teisingus rodiklius, apibūdinančius įmonėje vykstančius procesus. Priklausomai nuo dalykinės srities svarbu matuoti tuos parametrus, kurie suteikia daugiausiai informacijos apie veiklos sėkmingumą. Galima išskirti tam tikrus parametrus, kurie apibūdina, kokius kriterijus turi atitikti tam tikras apibendrintas matuojamas procesas (Jaquith, 2007):

- Matavimas turi būti susietas su piniginiais vienetais ir laiku;
- Turi būti gerai suprantamas viso kompanijos personalo;
- Turi būti plačiai naudojamas visoje industrijoje.

Pravartu į šiuos kriterijus atsižvelgti ir konstruojant informacijos saugoje vykstančių procesų metrikas.

2.1.1. Informacijos saugos metrikų samprata ir kokybės kriterijai

Rūpintis organizacijos saugumu yra būtina. Nuolatos pasitaikantys informacijos saugos incidentai tai patvirtina. Įvykus tiesioginiam įsilaužimui į organizacijos informacines sistemas patiriama didžiulė žala, įmonė dažnai nuskamba ir žiniasklaidoje, todėl susilaukiama ir netiesioginės žalos – reputacijos sumažėjimo. Tokie incidentai pasitaiko retai. Pakankamai dažnai už saugumą atsakingas asmuo įmonėje (CIO ar CISO) patiria neužtikrintumo jausmą, suvokdamas, kad organizacijos informacijos apsauga gali būti pažeista. Būtent metrikų naudojimas gali išspręsti šią padėtį. Teisingai sukonfigūruota metrikų sistema turėtų diagnozuoti informacijos saugos padėtį ir suteikti saugumo (Jaquith, 2007).

Metrikomis vadinami skaičių rinkiniai, kurie suteikia informaciją apie kokio nors proceso ar sistemos veikimą. Informacijos saugos metrikos – tai tarpusavyje susijusių dydžių visuma, leidžianti kiekybiškai įvertinti galimybę patirti žalą dėl neteisėto įsilaužimo į informacinę sistemą (Abbadi, 2006).

Informacijos saugos metrikos moksliniuose straipsniuose apibrėžiamos pakankamai skirtingai. Moksliniuose darbuose naudojamos informacijos saugos metrikų sąvokos ir apibrėžimai pateikiami 1 lentelėje:

1 lentelė. Moksliniuose darbuose naudojami informacijos saugos metrikų apibrėžimai (Yasasin & Schryen, 2015)

Nuoroda	**Darbe naudojamas informacijos saugos metrikos apibrėžimas**
(Hallberg et al., 2011)	Saugos metriką sudaro trys pagrindinės dalys: dydis, skalė ir interpretacija. Sistemų saugumo vertės matuojamos remiantis nurodytu dydžiu ir yra susietos su skale. Interpretacija nurodo, ką gautos konkrečios saugumo vertės reiškia.
(Jaquith, 2007)	Saugos metrikos yra grupė kertinių indikatorių, kurie apibūdina tiek autonominių, tiek nuo kitų sistemų priklausomų, informacijos saugos operacijų padėtį organizacijoje.
(Kaur & Jones, 2008)	Saugos metrikos suteikia struktūrą, kuri leidžia įvertinti į produktus įtrauktus saugos procesus ir komercines informacijos saugos paslaugas.
(Ouchani & Debbabi, 2015)	Saugos metrika tai kiekybinis dydis, atskleidžiantis apie konkrečios esybės saugumo lygį.
(Savola, 2007)	Saugos metrika yra kiekybinis ir objektyvus pagrindas saugos užtikrinimui. Ji palengvina verslo ir inžinerinius sprendimus susijusius su informacijos sauga.
(Julisch, 2009)	Saugos metrika yra priemonė, leidžianti pasiremti priimant informacijos saugos sprendimus ir tobulinti informacijos saugos valdymą.
(Chew et al., 2008)	Saugos metrikos tai įrankis, kuris leidžia palengvinti sprendimų priėmimą, pagerinti našumą ir atskaitomybę. Tai pasiekiama renkant, analizuojant ir pranešant atitinkamus, su informacijos saugos srities veikla susijusius, duomenis.

Pateikiami apibrėžimai rodo, kad informacijos saugos metrikos įvairiuose šaltiniuose apibrėžiamos skirtingai.

Informacijos saugos metrikos organizacijai gali suteikti nemažai naudos (Jaquith, 2007):

- Leidžia suprasti saugumo grėsmes;
- Leidžia pastebėti kylančias informacijos saugos problemas;
- Leidžia suprasti silpnąsias saugumo infrastruktūros vietas;
- Išmatuoja taikomųjų priemonių, kurios naudojamos saugumo problemoms spręsti, efektyvumą;
- Atskleidžia saugos technologijų ir procesų tobulinimo gaires.

Tam, kad organizacijos nesusidurtų su nesusipratimais ir keblumais manoma, kad metrikos turi būti paprastos ir lengvai suprantamos. Geromis metrikomis laikomos tos, kurios atitinka kriterijus (Jaquith, 2007):

- Tam tikras parametras yra nuolat matuojamas taikant tokią pačią metodiką;
- Lengvas ir nebrangus duomenų surinkimas;

- Išreiškiamos kaip skaitmuo arba procentine išraiška („aukštas“, „vidutinis“, „žemas“ - netinkama);
- Išreiškiamos įtraukiant tam tikrų standartinių matavimo vienetų (pvz.: laikas ar piniginė išraiška);
- Metrika turi būti specifinė, kalbanti apie konkretų procesą ir suteikianti aiškius duomenis tiems, kurie priima organizacinius sprendimus.

Nuolatos tokiais pačiais metodais matuojama metrika leidžia daryti išvadas ir gauti tokius pačius rezultatus (nepriklausomai nuo matuojančiojo asmens suvokimo ar daromų individualių prielaidų). Metrikos gavimas turi būti lengvas ir nebrangus. Duomenų surinkimas gali būti tiek labai paprasta, tiek ir pakankamai komplikuota užduotis. Kai kurioms metrikoms gauti, užtenka parašyti vieną SQL užklausą, o kitoms gali neužtekti ir atlikti begalę telefoninių skambučių. Manoma, kad viena iš geros metrikos savybių turėtų būti nesudėtingas duomenų, skirtų metrikai apskaičiuoti, gavimas. Taip pat svarbu, kad metrika būtų aiški ir suprantama, gerai apibūdintų tam tikrą procesą ir leistų priimti konkrečius sprendimus. Kaip pavyzdys metrika „vidutinis įmonės atakų skaičius“ yra pernelyg abstraktus, šiuo atveju reikėtų taikyti metriką „vidutinis atakų skaičius e-komercijos serveriams“. Tiksli metrika leis pritaikyti konkretesnius, saugumo problemą išspręsti galinčius, mechanizmus (Jaquith, 2007).

Tik žinodami, kokie parametrai apibūdina informacijos saugos metrikų kokybę, galime sukurti efektyvią metrikų sistemą. Tokia sistema leistų, su informacijos sauga susijusius sprendimus, priimti vadovaujantis skaitiniais parametrais. Šiuo metu dalyje organizacijų, sprendimai susiję su informacijos sauga, yra priimami tik vadovaujantis informacijos saugos ekspertų asmenine nuomone ir patirtimi. Ši situacija turėtų keistis, kadangi tai leistų smarkiai pagerinti informacijos saugos vadybos procesą. 141 specialistui iš įvairių pasaulio šalių, turinčių tiesioginį ryšį bei darbinę arba mokslinę patirtį, su informacijos saugos metrikomis buvo pateikta užduotis. Specialistams reikėjo iš 19 pagrindinių kokybės kriterijų, kurie apibūdina informacijos saugos metrikas, išrinkti svarbiausius. Šiuo tyrimu buvo siekiama išsiaiškinti pagrindinius kokybės kriterijus, kurie apibūdina gerą metriką. Tyrimo rezultatai parodė, kad anot respondentų svarbiausi yra trys pamatiniai kokybės kriterijai. Tai korektiškumas (angl. *correctness*), galimybė išmatuoti arba išmatuojamumas (angl. *measurability*) ir reikšmingumas arba prasmingumas arba reikšmingumas (angl. *meaningfulness*). Taip pat, kaip ketvirtas pagal svarbumą pažymimas kriterijus - gebėjimas panaudoti metriką (angl. *usability*). Korektiškumas reiškia, kad metrika yra korektiškai taikoma ir nesuteikia jokios klaidingos informacijos, metrika gaunama be klaidų. Išmatuojama metrika turi galimų reikšmių sritį, aiškų skaitiniais vienetais apibrėžtą dydį. Prasminga arba reikšminga metrika pateisina jai keliamus poreikius, o gebėjimas panaudoti apibūdina

metrikos teikiamą praktinę naudą. Šis tyrimas informacijos saugos specialistams suteikia aiškų suvokimą apie tai kas yra tikrieji kriterijai apibūdinantys metrikos kokybę (Savola, 2013).

Moksliniuose šaltiniuose galima rasti ir kitokius pagrindinius metrikas apibūdinančius kokybės kriterijus. Šie kokybės kriterijai pateikiami 2 lentelėje:

2 lentelė. Literatūroje išskiriami pagrindiniai informacijos saugos metrikų kokybės kriterijai (Yasasin & Schryen, 2015)

Nuoroda	**Pagrindiniai informacijos saugos metrikas apibūdinantys kriterijai**
(Jaquith, 2007)	• Tam tikras parametras yra nuolat matuojamas taikant tokią pačią metodiką • Lengvas ir nebrangus duomenų surinkimas, pageidautina automatiškai • Išreiškiamos įtraukiant tam tikrų standartinių matavimo vienetų • Metrika turi būti specifinė, kalbanti apie konkretų procesą ir suteikianti aiškius duomenis tiems, kurie priima organizacinius sprendimus
(Savola, 2013)	• Korektiškumas (angl. *correctness*) • Galimybė išmatuoti (angl. *measurability*) • Reikšmingumas (angl. *meaningfulness*) • Gebėjimas panaudoti metriką (angl. *usability*)
(Chew et al., 2008)	• Matavimai turi apimti kiekybinius duomenis (procentai, vidurkiai, skaičiai) • Matavimų duomenys turi būti lengvai gaunami • Turėtų būti matuojami tik besikartojantys informacijos saugos procesai • Matavimai turėtų būti naudingi, jie turėtų leistų sekti sistemų efektyvumą ir atlikti resursų skirstymą
(ISO/IEC, 2016)	Pateikiamos rekomendacijos apie informacijos saugos parametrų matavimą: • Duomenys lengvai surenkami • Skiriami žmogiški resursai, skirti duomenų surinkimui ir valdymui • Naudojami tinkami įrankiai • Potencialiai panašių indikatorių skaičius, paremtas baziniu matavimu • Lengvai interpretuojama • Matavimo rezultatų vartotojų skaičius • Matavimo tinkamumas ir matuojamos informacijos poreikis • Duomenų surinkimo, valdymo ir analizavimo kaštai

Remiantis skirtingais šaltiniais galima išgauti apibendrintus metrikų kokybės kriterijus. Toks apibendrinimas buvo pasiūlytas. Apibendrinus išskiriama, kad metrika turi būti: turinti skaitinius rėžius ar ribas, išreiškiama kiekybiškai, turinti tinkamus įvesties duomenis, patikima, pagrįsta, objektyvi, specifinė ir gaunama automatizuotai (Yasasin & Schryen, 2015).

Skirtinguose literatūros šaltiniuose išskiriami pakankamai panašūs pagrindiniai metrikos kokybės kriterijai. Tačiau galima įžvelgti ir skirtumų, todėl galima teigti, kad mokslo bendruomenė dar nėra galutinai sutarusi šiuo klausimu.

2.1.2. Informacijos saugos metrikų tipai ir pavyzdžiai

Saugos metrikas reikėtų skirstyti į tam tikras grupes pagal jų kilmę. Galima būtų išskirti tokią metrikų klasifikaciją kaip (Jaquith, 2007):

- Perimetro apsauga. Apibrėžia rizikas susijusias su galimais organizacijos saugos pažeidimais, kurie atkeliauja iš išorės (kalbama apie ugniasienes, IDS, el. laiškų analizę, darbuotojų atsparumą socialinės inžinerijos atakoms). Šio tipo metrikų pavyzdžiai pateikiami 3 lentelėje;
- Apimties ir valdymo sritis, kuri apibrėžia kaip sėkmingai organizacijoje sekasi įgyvendinti taikomą saugumo programą. Kitaip sakant ar numatytų saugumo programos veiksnių organizacijos viduje yra laikomasi. Nors CISO gali taikyti įvairiausius metodus, kurie tobulina informacijos saugumo parametrus įmonėje, realių galutinių taškų (pavyzdžiui, kompiuterių, serverių ar darbuotojų) šios priemonės gali ir nepasiekti. Šio tipo metrikų pavyzdžiai pateikiami 4 lentelėje;
- Informacijos pasiekiamumas ir sistemų patikimumas, kuris apibrėžia organizacijos pelną generuojančių sistemų veikimą apibūdinančias metrikas (pvz.: kalbama apie tokias metrikas kaip MTTR, MTBF). Šio tipo metrikų pavyzdžiai pateikiami 5 lentelėje.

Tai ne vienintelis metrikų klasifikavimo būdas. Egzistuoja ir kitokios metrikų klasifikacijos, kurios pateikiamos kituose moksliniuose darbuose. Pavyzdžiui, pagal įvesties duomenų tipą metrikos klasifikuojamos į: analizuojančios projektavimo ir kūrimo (angl. *design and build*) sritį, analizuojančios veikimo (angl. *operate*) procesus ir analizuojančius palaikymo ir atnaujinimo (angl. *maintain and update*). Projektavimas ir kūrimas apibūdina ir matuoja saugos inžinerinio proceso efektyvumą, informacinių sistemų kūrimą. Veikimo sritis apibūdina jau sukurtų ir veikiančių sistemų specifiką. Palaikymo ir atnaujinimo sritis apibūdina informacijos saugos valdymo efektyvumą, veikiančių procesų pasikeitimus (Julisch, 2009).

Galimas ir metrikų klasifikavimas taikant informacijos saugos valdymo standartus. Pavyzdžiui, ISO/IEC 27000 metrikų klasifikaciją galima atlikti remiantis standarto siūlomomis valdymo sritimis. Valdymo sritys aprašomos standarto 27001 dalyje, būtent ši klasifikacija bus taikoma ir tyrimo dalyje. Be to, pačiame standarte apibrėžiama, ir informacijos saugos stebėjimo, matavimų ir analizės dalis, tam skirtoje standarto dalyje – 27004 (ISO/IEC, 2016). Standarte aprašomi matavimų konstravimo pavyzdžiai ir galima klasifikacija, kurią apima 30 sričių. Keletas iš standarte siūlomų sričių: resursų skirstymas, politikų peržiūra, rizikos poveikis, auditavimo programa, slaptažodžių kokybė, apsauga nuo KPK, ugniasienės taisyklės, įrenginių konfigūracija, pažeidžiamumų aplinka ir kitos sritys (ISO/IEC, 2016).

Toliau pateikiami galimų ir organizacijose naudojamų metrikų pavyzdžiai. Metrikų skirstymui naudojama skyriaus pradžioje pasiūlyta klasifikacija:

3 lentelė. Informacijos saugos metrikų lentelė. Perimetro apsauga (Jaquith, 2007)

Metrikos pavadinimas, matavimo vienetas	**Metrikos apibūdinimas, parametro stebėjimo tikslas**	**Sistema, generuojanti metriką (šaltinis)**
El. paštas		
Per dieną ateinančių žinučių skaičius, (vnt.)	Įprasto el. laiškų srauto stebėjimas	El. laiškų sistema
Aptikto šlamšto (angl. *spam*) kiekis, (vnt., %)	El. laiškų užterštumo rodiklis	El. laiškų filtravimo sistema
Neaptikto šlamšto (angl. *spam*) kiekis (vnt., %)	El. laiškų filtravimo sistemos efektyvumą apibūdinantis rodiklis	El. laiškų filtravimo sistema
Klaidingai teigiamas (angl. *false positive*) šlamšto aptikimas (vnt., %)	El. laiškų filtravimo sistemos efektyvumą apibūdinantis rodiklis	El. laiškų filtravimo sistema
Šlamšto aptikimo klaidos, į kurias patenka klaidingai teigiami bei neaptikti kenksmingi laiškai (%)	El. laiškų filtravimo sistemos efektyvumą apibūdinantis rodiklis	El. laiškų filtravimo sistema
Aptiktų virusų ir šnipinėjančio KPK skaičius (vnt., %)	Parodo el. laiškų užterštumą KPK	El. laiškų filtravimo sistema
Antivirusinė programinė įranga		
Virusai ir šnipinėjantis KPK aptiktas vartotojų lankomuose internetiniuose puslapiuose (vnt., %)	Atskleidžia vartotojų polinkį lankytis interneto svetainėse, turinčiose KPK	Perimetro filtravimo programinė įranga
KPK aptiktas (vnt.): • Serveriuose; • Stacionariuose kompiuteriuose; • Nešiojamuose kompiuteriuose;	Atskleidžia virusais ir kitokiu KPK infekuotos aparatinės įrangos skaičių	Antivirusinė programinė įranga
Virusai ir KPK incidentai, reikalaujantys išvalyti sistemą (vnt., % lyginant su visais KPK incidentais)	Parodo kiek resursų skiriama KPK valymui	Antivirusinė programinė įranga; Problemų bilietų sistema; Rankiniai duomenų šaltiniai.
Šnipinėjančio KPK incidentų valymui skirtos lėšos • Grupuojama pagal organizacijos skyrius	Parodo kiek finansų yra išleidžiama atliekant valymo darbus	Antivirusinė programinė įranga; Problemų bilietų sistema; Rankiniai duomenų šaltiniai.
Virusų ir KPK incidentų valymui skirtos išlaidos • Grupuojama pagal organizacijos skyrius	Parodo kiek finansų yra išleidžiama atliekant valymo darbus	Antivirusinė programinė įranga; Problemų bilietų sistema; Rankiniai duomenų šaltiniai.
Iš organizacijos tinklo užfiksuoto siunčiamo KPK skaičius (vnt.)	Atskleidžia organizacijos infekuotų įrenginių skaičių	El. laiškų turinio filtravimo sistema

Ugniasienė ir tinklo perimetras		
Metrikos pavadinimas, matavimo vienetas	**Metrikos apibūdinimas, parametro stebėjimo tikslas**	**Sistema, generuojanti metriką (šaltinis)**
Ugniasienės taisyklių pakeitimai (vnt.) • Grupuojama pagal organizacijos skyrius • Grupuojama pagal grupės serverio tipą	Atskleidžia koks yra saugumo sudėtingumas	Ugniasienės valdymo sistema; Laiko sekimo ir apmokestinimo už paslaugas sistemos.
Ugniasienės eksploatavimui reikalingi darbo ištekliai (praleistas laikas val.)	Parodo, kiek laiko praleidžiama dirbant prie ugniasienės poreikių	Žmonių resursų valdymo sistema; Rankiniai duomenų šaltiniai.
Ateinantys prisijungimai/sesijos prie organizacijos internete esančių serverių (vnt.)	Atskleidžia ateinančio vartotojų srauto dydį	Ugniasienės valdymo sistema
Atvirų bevielio ryšio taškų skaičius (angl. *open wireless access points*)	Atskleidžia potencialų pažeidžiamumą prieš išorines atakas	Bevielio ryšio skenavimo įrankiai
Tinklo įrenginiai, tiesiogiai prisijungę prie esminių transakcijų ir finansinių sistemų, be tarpinių ugniasienių (vnt.)	Atskleidžia potencialų pažeidžiamumą atakoms	Kompiuterinio tinklo diagramos; Kompiuterinio tinklo žemėlapį braižanti programinė įranga (angl. *network mapping software*).
Atakos		
Internetu atliekamų atakų klasifikavimas į tris įvykių pavojingumo lygius (%): • Tikėtinos atakos (generuojamas pradinis IDS įvykis); • Įtariamieji (mašininiu būdu išfiltruoti atakų pranešimai); • Atakuojantys (rankinis darbuotojų atliekamas tyrimas);	Atskleidžia atakų pavojingumo lygį	IDS; Ugniasienė; Problemų bilietų sistema; Rankiniai duomenų šaltiniai.
Atakų skaičius (vnt.)	Absoliutus atakų skaičius, tiek sėkmingų, tiek nesėkmingų	IDS; Rankiniai duomenų šaltiniai.
Sėkmingų atakų skaičius (vnt., %)	Atskleidžia perimetro apsaugos priemonių efektyvumą	IDS; Rankiniai duomenų šaltiniai.

4 lentelė. Informacijos saugos metrikų lentelė. Apimties ir valdymo sritis (Jaquith, 2007)

Antivirusinė programinė įranga		
Metrikos pavadinimas, matavimo vienetas	**Metrikos apibūdinimas, parametro stebėjimo tikslas**	**Sistema, generuojanti metriką (šaltinis)**
Kompiuterinės darbo vietos, serveriai turintys antivirusinę programinę įranga	Antivirusinės programinės įrangos apimtis	Antivirusinė programinė įranga; Tinklo valdymo sistema
Kompiuterinės darbo vietos ir serveriai turintys naujausius KPK duomenų bazės sąrašus	Antivirusinės programinės įrangos paslaugos efektyvumas	Antivirusinė programinė įranga
Programinės įrangos kritinių atnaujinimų valdymas (angl. *patch management*)		
Aparatinė įranga negavusi kritinių programinės įrangos atnaujinimų (%). Grupuojama pagal aparatinės įrangos tipą.	Atskleidžia apie programinės įrangos atnaujinimo spragas	Programinės įrangos atnaujinimo valdymo sistema Pažeidžiamumų valdymo sistema
Per tam tikrą laiko tarpą pritaikytų ir nepritaikytų kritinių atnaujinimų skaičius (vnt.)	Atskleidžia programinės įrangos atnaujinimo proceso vykdymo efektyvumą	Programinės įrangos atnaujinimo valdymo sistema
Vėlavimas atlikti kritinį saugumo atnaujinimą (laikas)	Parodo, kaip greitai įrašomi kritiniai saugumo atnaujinimai	Programinės įrangos atnaujinimo valdymo sistema
Tinklo įrenginių konfigūracija (angl. *host configuration*)		
Metrikos pavadinimas, matavimo vienetas	**Metrikos apibūdinimas, parametro stebėjimo tikslas**	**Sistema, generuojanti metriką (šaltinis)**
Sistemų atitinkančių apibrėžtą konfigūraciją procentinė dalis (%)	Parodo organizacijos sistemų atitikimą konfigūracijos standartui	Kompiuterių valdymo sistema (angl. *desktop management software*) Pasikeitimų kontrolės programinė įranga (angl. *change control software*)
Galimybė valdyti sistemas per nuotolį (%)	Sistemos, kurios gali būti valdomos ir administruojamos per nuotolį	Sistemų valdymo programinė įranga; Programinės įrangos atnaujinimo valdymo sistema; Antivirusinė programa.
Aktyviai stebimos kritinės organizacijos sistemos (%)	Veikimo laiko ir saugos stebėjimo valdymo kontrolės efektyvumas	SIEM

Pažeidžiamumų valdymas		
Metrikos pavadinimas, matavimo vienetas	**Metrikos apibūdinimas, parametro stebėjimo tikslas**	**Sistema, generuojanti metriką (šaltinis)**
Pažeidžiamumus skenuojanti programine įranga padengiamos sistemos (%)	Parodo pažeidžiamumus skanuojančios programinės įrangos efektyvumą	Pažeidžiamumus skenuojanti programinė įranga
Randamų pažeidžiamumų skaičius per fiksuotą laiko vienetą (vnt.)	Apibūdina kokiais kiekiais yra randami pažeidžiamumai ir ar šis skaičius bėgant laikui keičiasi	Pažeidžiamumus skenuojanti programinė įranga
Laikas skiriamas pažeidžiamumo sutvarkymui	Charakterizuoja kaip greitai yra taisomos spragos, pažeidžiamumai sistemose	Pažeidžiamumus skenuojanti programinė įranga; Problemų bilietų sistema.

5 lentelė. Informacijos saugos metrikų lentelė. Informacijos pasiekiamumas ir sistemų patikimumas (Jaquith, 2007)

Metrikos pavadinimas, matavimo vienetas	**Metrikos apibūdinimas, parametro stebėjimo tikslas**	**Sistema, generuojanti metriką (šaltinis)**
Veikimo laikas (angl. *uptime*)		
Sistemų veikimo laikas (laikas, %)	Kritinių sistemų prieinamumo matavimas	Sistemų stebėjimo programinė įranga; Rankinis sekimas.
Neplanuotas veiklos sutrikimas bei neplanuotas veiklos sutikimas, dėl saugos incidentų (%, laikas)	Matuojama, kiek laiko tam tikra sistema buvo neplanuotai sutrikusi, išskiriami atvejai dėl saugos incidentų	Specializuotos skaičiuoklės; Rankinis sekimas.
MTBF (laikas)	Parodo, kaip dažnai sistemos elementai neveikia	Specializuotos skaičiuoklės; Rankinis sekimas.
Sistemos atstatymas (angl. *system recovery*)		
Personalo reakcijos laikas (vidutinis laikas)	Vidutinis laikas, skaičiuojamas nuo sistemos gedimo iki pradėjimo sistemą taisyti	Specializuotos skaičiuoklės
MTTR (laikas)	Parodo, kiek laiko reikia tam, kad neveikiantis sistemos elementas būtų sutvarkytas	Specializuotos skaičiuoklės; Rankinis sekimas.
Produkcinės sistemos pakeitimų kontrolė (angl. *change control*)		
Pakeitimų skaičius, tam tikrame laiko tarpe (vnt.)	Parodo periodinį pakeitimų skaičių produkcinėje aplinkoje	Pakeitimų valdymo programinė įranga
Pakeitimai, atlikti taikant išimtis, per tam tikrą laiko tarpą	Parodo periodinį pakeitimų, atliekamų taikant išimtis, skaičių produkcinėje aplinkoje	Pakeitimų valdymo programinė įranga

Metrikos pavadinimas, matavimo vienetas	Metrikos apibūdinimas, parametro stebėjimo tikslas	Sistema, generuojanti metriką (šaltinis)
Pakeitimų pažeidimai, tyčia pažeidžiant pakeitimų taisykles	Atskleidžia kaip dažnai pakeitimų kontrolės taisyklės būna pažeidžiamos	Pakeitimų valdymo programinė įranga

3, 4 ir 5 lentelėse pateiktos informacijos saugos metrikos yra vienos reikšmingiausių, plačiai naudojamos informacijos saugos industrijoje. Žinoma egzistuoja ir kitokios metrikos, kurios sėkmingai taikomos įvairiose informacijos saugos procesus stebinčiose organizacijose. Informacijos saugos metrikų sąvoka galima prilyginti verslo valdymo srityje taikomiems KPI. KPI tikslas – apibendrinti prasmingai prilygintus duomenis (Peterson, 2006).

2.1.3. Agreguotos informacijos saugos metrikos

Skyriuje 2.1.2 pateikiamos klasikinės informacijos saugos metrikos. Jos susideda iš vieno dydžio arba vieno kintamojo. Kaip pavyzdys metrika – organizacijos serveriuose per dieną aptikto KPK skaičius, kuris matuojamas vienetais. Tai vieno kriterijaus metrika. Sudėjus bent dvi skirtingas metrikas ir įvertinus, jų svarbą apibūdinančius svorio koeficientus, galime gauti apibendrintą dydį. Būtent tai vadiname agreguota arba daugiakritere informacijos saugos metrika.

Nagrinėtuose informacijos saugos problemas tiriančiuose straipsniuose agreguotų informacijos saugos metrikų sąvoka nėra nusistovėjusi. Mokslininkai siūlo įvairias metodikas informacijos saugos padėties vertinimui organizacijoje taikant metrikas. Viename iš straipsnių pateikiama netradicinė daugiakriterė informacijos saugos metrika, skirta įvertinti apibendrintą duomenų bazių valdymo sistemos saugą. Tai atliekama matuojant neužtikrintumą, kuris kyla dėl galimų atakų prieš duomenų bazių valdymo sistemas. (Neto & Vieira, 2011).

Moksliniuose straipsniuose taip pat diskutuojama apie agreguotų informacijos saugos metrikų prasmę. Teigiama, kad atskirų saugos metrikų agregavimas yra naudingas, tačiau to atlikimas nėra paprastas procesas. Norint metrikas agreguoti, tam, kad būtų gauta viena apibendrinta, yra būtina įvertinti priklausomybes tarp jų. Priklausomybių įvertinimas yra sprendimo priėmimo uždavinys, kadangi reikia nuspręsti kiek tam tikras matuojamas veiksnys yra svarbus kitų atžvilgiu (Pendleton et al., 2016). Tai atlikti galima įvedant svorio koeficientus, kurie apibrėžtų tradicinių metrikų reikšmę agreguotoje, daugiakriterėje metrikoje.

Mokslo bendruomenėje agreguotų metrikų problema dar nėra nagrinėjama plačiai, todėl nėra sutarta dėl apibendrintos sąvokos. Verslo įstaigoms agreguotų metrikų naudojimas yra pasitaikantis reiškinys. Tokias, agreguotas, apibendrintą informaciją apie konkrečių veiklos sričių informacijos saugą teikiančias, metrikas savo klientams siūlo verslo įstaigos (Tijink Gerwin et al., 2019).

2.2. Daugiakriteriai sprendimų priėmimo metodai

Pastarąjį dešimtmetį MCDA naudojama labai plačiai. Tai patvirtina įvairūs moksliniai darbai (Bhol et al., 2020; Chakraborty et al., 2015; Singh & Pattnaik, 2018; Solana-González et al., 2019). Taip pat darbais siekiama tiek patobulinti esamus įvairių sričių taikomus metodus, tiek sukurti naujus (Velasquez & Hester, 2013). Šiame skyriuje bus aptartos daugiakriterių tyrimų metodikos, aprašyta jų klasifikacija, pateiktas palyginimas, skirtingų metodų privalumai ir trūkumai.

2.2.1. Daugiakriterių sprendimų priėmimo metodų samprata ir klasifikacija

Daugiakriteriai sprendimų priėmimo metodai yra naudojami siekiant priimti patį optimaliausią sprendimą. MCDM yra gerai žinomas daugiakriteris metodologinis būdas, taikomas priimant sprendimus. Šis būdas taikomas įvairiose mokslo ir verslo srityse, kurias apima tiek vadybinių mokslų sritis, tiek inžinerija bei IT.

Prieš gilinantis į konkrečius problemų sprendimo metodus, svarbu išsiaiškinti šiems metodams būdingą klasifikavimą. Metodų klasifikavimas atliekamas remiantis skirtingais veiksniais. MCDM skirstomi į dvi grupes: daugiaobjekčius, MODM (angl. *Multi Objective Decision Making*) ir daugiatikslius, MADM (angl. *Multi Attribute Decision Making*). Daugiatiksliai metodai toliau klasifikuojami pagal duomenų, naudojamų alternatyvų rangavimui, tipą. Metodai klasifikuojami į deterministinius, stochastinius (tikimybinius) ir neapibrėžtų aibių (angl. *fuzzy*). Pagal procese dalyvaujančių sprendimo priėmėjų skaičių, metodus galima suskirstyti į vieno žmogaus sprendimo arba grupės sprendimo metodus (Poškas et al., 2012; Simanavičienė, 2011). Siūlomos ir kitokios daugiakriterių metodų klasifikacijos, pagal informacijos, kuri pateikiama sprendimų priėmėjams tipą. Pagal šią klasifikaciją galima išskirti rangų koreliacijos metodus, pirmenybių palyginimu (prioritetiškumu) paremtus metodus, metodus, leidžiančius kokybinius vertinimus paversti kiekybiniais bei metodus apskaičiuojančius atstumą nuo atskaitos taško (Keršulienė et al., 2010).

Sprendžiant MCDM uždavinius dažnai susiduriama su kokybiniais kriterijais. Tokioms problemoms spręsti naudojamas ekspertinis vertinimas. Tradiciniuose MCDM metoduose žmonių priimami sprendimai yra paverčiami konkrečiomis skaitinėmis vertėmis. Tačiau neretai, sprendimų priėmėjams yra sunku apsispręsti dėl tikslios tam tikros problemos skaitinės vertės (Kahraman et al., 2014). Tokiu atveju galima naudoti neapibrėžtų aibių (angl. fuzzy) metodus.

2.2.2. Daugiakriterių sprendimų priėmimo metodų palyginimas

Egzistuoja įvairūs skirtingomis savybėmis pasižymintys daugiakriteriai sprendimų priėmimo metodai. Vieni dažniausių ir taikomų labai plačiai yra (Poškas et al., 2012; Velasquez & Hester, 2013):

- Analitinis hierarchinis procesas (angl. *Analytic Hierarchy Process – AHP*); AHP pagrįstas sprendimo priėmėjų vertinimu, siekiant išskaidyti sudėtingą problemą į hierarchiją su pagrindiniu tikslu

aukščiausiame lygmenyje, kriterijais tarpiniuose lygmenyse ir sprendimo alternatyvomis, pačiame žemiausiame hierarchijos lygmenyje (Wang et al., 2016);

- Neapibrėžtų aibių metodas (angl. *Fuzzy*);
- *SAW* (angl. *simple additive weighting*) – paprastų svorių sudėjimo metodas. Dalyje literatūros dar vadinamas *WSM* (angl. *Weighted Sum Model*) arba *WPM* (angl. *Weighted Product Model*). Šiuose metoduose alternatyvos balas yra lygus pagal vertinimo reitingus pasvertai sumai (Wang et al., 2016);
- Prioritetiškumo (angl. *Outranking*) metodai – *ELECTRE* (angl. *Elimination and Choice Expressing REality*) ir *PROMETHEE* (angl. *Preference Ranking Organization Method for Enrichment Evaluations*);
- *TOPSIS* (angl. *Technique for Order Preference by Similarity to Ideal Solution*). Metodas paremtas idėja, jog geriausias sprendimas turėtų būti arčiausiai idealaus sprendimo ir toliausiai nuo ne idealaus sprendimo (Wang et al., 2016);
- *Fuzzy TOPSIS* – tai *TOPSIS* metodo pritaikymas neapibrėžtai aplinkai (Chen, 2000);
- *MAUT* (angl. *Multi Attribute Utility Theory*). Metodas remiasi naudingumų skaičiavimais, kas leidžia priimti optimaliausią sprendimą. Skaičiuojant įtraukiami tokie parametrai kaip neapibrėžtumas, neužtikrintumas (angl. *uncertainty*) (Velasquez & Hester, 2013);
- *DEA* (angl. *Data Envelopment Analysis*) – Duomenų gaubtinės analizės metodas. Metodas sprendimą apibūdina matuodamas rezultatų ir išteklių santykį (Wang et al., 2016);
- *GP* (angl. *goal programming*) – tai pragmatiškas metodas, leidžiantis pasirinkti iš neriboto skaičiaus alternatyvų (Velasquez & Hester, 2013);
- *CBR* (angl. *Case-Based Reasoning*) – yra metodas, kurio esmė iš turimos duomenų bazės išgauti atvejus, kurie pasiūlytų problemos sprendimą (Velasquez & Hester, 2013);
- *SMART* (angl. *Simple-Multi Attribute Rating Technique*) – kiek paprastesnė MAUT versija (Velasquez & Hester, 2013);
- *WASPAS* (angl. *weighted aggregated sum product assessment*) – svertinės agreguotos sumos daugybos metodas, kuris yra sudarytas iš dviejų metodų: *WSM* (angl. *weighted sum model*) ir *WPM* (angl. *weighted product model*) (Zavadskas et al., 2012).

Metodai yra pakankamai skirtingi, visi turi savo privalumų ir trūkumų. Dėl šių skirtumų yra pakankamai sunku atlikti objektyvų šių metodų palyginimą. Apibendrintas dalies aprašytų metodų palyginimas pateikiamas 6 lentelėje:

6 lentelė. Daugiakriterių metodų palyginimas (Poškas et al., 2012)

	AHP	***Fuzzy***	***WSM***	***WPM***	***ELECTRE PROMETHEE***	***TOPSIS***	***MAUT***
Pasaulinė praktika inžineriniams. MCDA uždaviniams spręsti	+	+/-	-	-	+/-	+/-	+/-
Grupinis sprendimų priėmimas	+/-	+	+	+	+/-	+/-	+/-
Naudoja hierarchinę uždavinio struktūrą	+	-	-	-	-	-	-
Užtikrina įverčių suderinamumą	+	-	-	-	+	+	+
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

Moksliniuose inžinerinės krypties straipsniuose labai dažnai taikomas AHP metodas (Poškas et al., 2012; Solana-González et al., 2019). Šis metodas naudoja hierarchinę uždavinio struktūrą, suskaldo problemą į mažesnes dalis, todėl įvertina ir visus problemos aspektus (Poškas et al., 2012).

MCDM metodų apibendrinimas taip pat pateikiamas ir 7 lentelėje. Lentelėje aprašomi metodų privalumai ir trūkumai bei dažniausiai pasitaikančios panaudojimo sritys.

7 lentelė. MCDM metodų apibendrinimas (Siksnelyte-Butkiene et al., 2020; Velasquez & Hester, 2013)

Metodas	**Privalumai**	**Trūkumai**	**Panaudojimo sritys**
MAUT	Įvertina neapibrėžtumą, gali būti įtraukti pageidavimai.	Reikalauja daug duomenų; pageidavimai turi būti labai tikslūs.	Ekonomika, finansai, aktuarinis skaičiavimas, agrokultūra, energetika.
AHP	Lengva naudoti; pritaikomas pagal dydį, hierarchinė sistema gali būti pritaikyta taigi būtų galima nagrinėti įvairias problemas; nereikalauja daug duomenų.	Problemos dėl tarpusavio priklausomybių tarp kriterijų ir alternatyvų; gali vesti į neatitikimus tarp sprendimų ir reitingavimo kriterijų; reitingo pasikeitimai.	Efektyvumo problemoms spręsti, resursų planavimui, organizacijos politikoje ir strategijoje, viešojoje politikoje.
CBR	Nereikalauja daug duomenų; nereikalauja daug priežiūros; gali tobulėti bėgant laikui; gali prisitaikyti prie aplinkos pasikeitimo.	Jautrus nenuosekliems duomenims; reikalauja daug atvejų.	Verslai, transporto priemonių draudimas, medicina ir inžinerija.

Metodas	Privalumai	Trūkumai	Panaudojimo sritys
DEA	Gali susidoroti su daug įvesčių ir išvesčių; efektyvumas gali būti analizuojamas ir įvertintas kiekybiškai.	Nesusitvarko su netiksliais duomenimis; daro prielaidą, kad visi įeinantys ir išeinantys dydžiai yra tikslūs ir gerai žinomi.	Ekonomika, medicina, kelių sauga, komunalinės paslaugos, agrokultūra, pardavimų ir verslo problemų sprendimas.
Fuzzy	Priima netikslius duomenis; atsižvelgia į nepakankamą informaciją.	Sunku sukurti ir išplėtoti; gali reikalauti didelio kiekio simuliacijų prieš realų naudojimą ir rezultatus.	Inžinerija, ekonomika, aplinkosauga, medicina ir vadyba.
SMART	Paprastas metodas; įgalina bet kokio tipo svorių priskyrimo technikas; mažiau pastangų reikia įdėti priimantiems sprendimus.	Vertinant metodo struktūrą, procedūra gali būti nepatogi.	Aplinkosauga, statybų sektorius, logistika, krašto apsauga, gamybinės ir surinkimo problemos.
GP	Gali susitvarkyti su didelės apimties problemomis; gali sukurti didelį kiekį alternatyvų.	Koeficientų svorių sistema; paprastai naudojamos kiti MCDM metodai, tam, kad įgyti svorių koeficientus.	Gamybos planavimas, tvarkaraščio sudarymas, medicina, portfelio pasirinkimas, energetika.
ELECT-RE	Vertina neužtikrintumą ir neapibrėžtumą.	Procesą ir jo rezultatą sunku apibūdinti paprastais žodžiais; prioritetiškumas neleidžia tiesiogiai identifikuoti alternatyvų stiprybių ir silpnybių.	Energetika, ekonomika, aplinkosauga, logistikos problemų sprendimas.
PROME-THEE	Lengvas naudojimas; nereikalauja prielaidos, kad kriterijai yra proporcingi.	Neteikia aiškaus metodo, kuriuo būtų galima paskirstyti svorius.	Aplinkosauga, hidrologija, verslas ir finansai, logistika, gamyba, energetika, agrokultūra.
SAW	Gebėjimas kompensuoti kriterijus; intuityvus sprendimo priėmėjams; skaičiavimai paprasti, nereikalauja sudėtingos programinės įrangos.	Apskaičiavimai ne visada atskleidžia realią situaciją; gauti rezultatai gali būti nelogiški.	Verslas ir finansinių institucijų valdymas.
TOPSIS	Paprastas procesas; lengvas naudojimas ir programavimas; metodo atlikimo žingsnių skaičius išlieka toks pat, nepriklausomai nuo atributų skaičiaus.	Euklido atstumas neįvertina atributų koreliacijos; sunku pasverti ir išlaikyti sprendimo pastovumą. Metodas tinkamas, kai alternatyvų indikatoriai neturi labai didelių skirtumų. Esant skirtumams gali būti iškreipti galutiniai rezultatai.	Tiekimo grandinės valdymas ir logistika, inžinerija, gamyba, verslas ir marketingas, aplinkosauga, žmogiškieji resursai.
WASPAS	Aukštas patikimumo lygis (Stojić et al., 2018) Pakankamai lengvas skaičiavimo procesas.	Metodas įvertina tik minimalias (ne naudingiems kriterijams) ir maksimalias (naudingiems kriterijams) vertes. Ne visos alternatyvų vertės yra įvertinamos.	Inžinerija, gamyba, verslas

Konkretaus uždavinio sprendimui būtina pasirinkti tinkamiausią metodą. Ši užduotis yra pakankamai sudėtinga, kadangi reikia įvertinti metodo ir sprendžiamos problemos atitikimą. Atlikus teisingą pasirinkimą ir sėkmingai pritaikius metodą, tyrime gauti rezultatai turėtų būti teisingi ir patikimi.

2.3. Moksliniuose darbuose naudojami informacijos saugos metrikų vertinimo, optimizavimo ir tobulinimo metodai

Informacijos saugos metrikos informacijos saugos valdymo srityje yra taikomos jau pakankamai ilgą laiką. Mokslinė bendruomenė atlieka įvairius tyrimus susijusius su informacijos saugos metrikomis. Dažnai pasitaiko tyrimai, kuriais siekiama išsiaiškinti pagrindinius informacijos saugos metrikų vertinimo kriterijus (R. K. A. Ahmed, 2016; Savola, 2013). Atliekami ir įvairūs tyrimai, kurių tikslas sudaryti metrikų klasifikaciją, taksonomiją (Julisch, 2009; Purboyo et al., 2011; Savola, 2007). Kita dalis mokslinių straipsnių siekia informacijos saugos metrikas įvertinti, optimizuoti, patobulinti (Bodeau et al., 2018; Ramos et al., 2017; Yasasin & Schryen, 2015; Yee, 2019). Būtent ši metrikas analizuojančių straipsnių dalis yra pati aktualiausia, sutampanti su šio darbo pagrindiniu tikslu – informacijos saugos metrikų tobulinimu.

Saugos metrikos nėra standartizuotos ir tai vis dar yra pakankamai sudėtingas uždavinys (Yee, 2019). Mokslininkų bendruomenė siūlo įvairius metodus skirtus metrikų tobulinimui ir optimizavimui. Vienas iš būdų atskirti geras metrikas nuo blogų yra taikyti iš anksto paruoštą metodiką, kurios esmė atsakyti į metrikas apibūdinančius klausimus. Teigiami atsakymai į visus klausimyno klausimus reikštų, kad analizuojama metrika yra gera. Žinoma toks metodas reikalauja didelės vertinančio asmens ar asmenų grupės kompetencijos ir yra priklausomas nuo konkretaus, sprendžiančio asmens, požiūrio (Yee, 2019). Kitas siūlomas metrikų patikrinimo metodas yra labai panašus. Tyrime taikant S. Toulmin‘o argumentavimo metodą buvo susisteminti įvairių autorių siūlomi metrikos kokybės kriterijai. Susisteminti kriterijai tapo metrikos patikrinimo klausimynu, kuriuo remiantis analizuojama metrika. Į šiuos klausimus pateikus teigiamus atsakymus, įsitikiname metrikos kokybe (Yasasin & Schryen, 2015).

Atliekami tyrimai ir susiję su kibernetinio atsparumo (angl. *cyber resilience*) metrikomis. Kibernetinis atsparumas yra apibrėžiamas kaip gebėjimas nenutrūkstamai pasiekti numatytus rezultatus, nepaisant neigiamų kibernetinių įvykių (Björck et al., 2015). Informacijos saugos metrikos iš dalies apima ir kibernetinio atsparumo metrikų sritį. Pasiūlyti kibernetinio atsparumo metrikų tobulinimo metodai yra aktualūs ir informacijos saugos metrikoms. Atliekant kibernetinio atsparumo metrikų pasirinkimą siūloma įvertinti daug kriterijų. Tam, kad metrika būtų tinkama pasirinkimui, visų pirma turi būti įmanoma ją įvertinti. Taip pat turi būti įmanoma greitai išgauti metrikai sudaryti reikalingus duomenis. Metrikos teikiama nauda privalo viršyti jos gavimo ir sudarymo metu patiriamus nuostolius. Keliami ir kitokie reikalavimai, kuriuos turi atitikti pasirenkama metrika. Metrikos pasirinkimo kriterijai turėtų būti sudėlioti pagal prioritetiškumą, kuris gali

skirtis priklausomai nuo konkrečios organizacijos poreikių. Kibernetinio atsparumo metrikų vertinimui siūloma metrikų specifikacija. Ji leidžia įvertinti kaip konkreti metrika gali būti panaudota, kokios yra metrikos verčių reikšmės arba kokią informaciją konkreti skaitinė vertė suteikia (Bodeau et al., 2018).

Informacijos saugos valdymo srityje nevengiama taikyti MCDM metodų. Galima rasti mokslinių straipsnių tyrinėjančių informacijos saugos valdymo sritį – atitikimą keliamiems saugumo standartams. Šiai problemai spręsti naudojamas MCDM. Pasirenkamas AHP metodas, kuriuo gaunamas kriterijų prioritetiškumo sąrašas (Solana-González et al., 2019). Taip pat MCDM metodai taikomi informacijos saugos metrikų įvertinimui (Bhol et al., 2020).

Mokslinėje literatūroje galima rasti ir straipsnių, kuriuose informacijos saugos metrikų vertinimui naudojami MCDM metodai. Taikant du populiarius MCDM metodus – AHP ir ELECTRE III buvo atlikta informacijos saugos metrikų analizė, pagal keturis parametrus: jautrumą (angl. *susceptibility*), apsaugos mechanizmus (angl. *protection mechanism*), rizikos išmatavimą (angl. *risk measurement*) ir susikirtimus (angl. *encounters*). Pagal šiuos keturis parametrus buvo lyginamos trijų kompanijų informacijos saugos metrikos. Abu (AHP ir ELECTRE III) daugiakriteriai sprendimų priėmimo metodai parodė tokius pačius rezultatus, buvo sudarytas kompanijų reitingas (nuo geriausios iki blogiausios) (Bhol et al., 2020). Aptarto mokslinio darbo tematika yra kiek pakankamai panaši į šio darbo tematiką. Pagrindinis skirtumas, kad tyrimu buvo siekiama įvertinti naudojamas kompanijų metrikas, o ne pasiūlyti agreguotas informacijos saugos metrikas, kas yra šio mokslinio darbo apimtyje. Kitame darbe kalbama apie kompiuterinio tinklo saugos metrikas, kurios leidžia sužinoti apibendrintą situaciją apie tinklo atsparumą atakoms. Pasiūlomas metrikų apibendrinimas, jų klasifikavimas taip pat užsimenama apie agreguotos metrikos sąvoką, kuri leistų apibendrinti atskiromis metrikomis surenkamą informaciją (Ramos et al., 2017). Egzistuoja ir darbai kurių tikslas pasiūlyti metrikų agregavimo architektūrą, nurodyti kokiu būdu galima įgyvendinti metrikų agregavimo procesą (Y. Ahmed et al., 2018).

Pagrindinis šio darbo tikslas yra prisidėti prie informacijos saugos metrikų tobulinimo, pasiūlant naujas, agreguotas metrikas. Šių metrikų taikymas galės netiesiogiai prisidėti prie organizacijų informacijos saugos padėties pagerėjimo.

2.4. Apžvalgos apibendrinimas, išvados ir tolimesni darbai

Šiame skyriuje buvo aprašytos šiuo metu organizacijose naudojamos informacijos saugos metrikos. Taip pat panagrinėti daugiakriteriai sprendimų priėmimo metodai. Apžvelgti moksliniai straipsniai susiję su informacijos saugos metrikomis, taip pat moksliniai straipsniai, kurių tikslas įvertinti, optimizuoti ar tobulinti informacijos saugos metrikas.

Pradinė mokslinių straipsnių ir tyrimų analizė parodė, kad informacijos saugos valdymo srityje daugiakriterių sprendimo priėmimo (MCDM) metodų naudojimas yra pakankamai dažnas (Bhol et al., 2020; Solana-González et al., 2019).

Taip pat atlikta pradinė mokslinių straipsnių ir tyrimų analizė parodė, kad metrikų tobulinimas ir optimizavimas įprastai atliekamas pasiūlant metodą kaip įvertinti konkrečios metrikos kokybę. Dažnai sudaromas tam tikras klausimynas arba parametrų, kuriuos turi atitikti metrika, sąrašas (Bodeau et al., 2018; Yasasin & Schryen, 2015; Yee, 2019). Mokslinėje literatūroje stinga straipsnių, kuriuose būtų siūlomos metodikos skirtos metrikų tobulinimui, ar būtų išskiriamos specifinės rekomenduojamos metrikos.

Apibendrinus atliktą literatūros analizę formuluojamos tolimesnės tyrimo išvados:

1. Autoriai siūlo naudojamos informacijos saugos metrikos skirstyti į keletą sričių. Vienas iš galimų skirstymo pavyzdžių: susijusios su perimetro apsauga, apimties ir valdymo sritimi bei informacijos pasiekiamumu ir sistemų patikimumu (Jaquith, 2007).
2. Egzistuoja skirtingi daugiakriteriai sprendimų priėmimo metodai. Svarbu atlikti teisingą šio metodo pasirinkimą, kadangi nuo to gali priklausyti ir tyrime gauti rezultatai.
3. Atlikus literatūros šaltinių, susijusių su informacijos saugos metrikų tobulinimu, analizę, buvo pastebėta, kad moksliniuose darbuose bandoma paruošti metodikas metrikų įvertinimui, tačiau ne tobulinimui. Agreguotų metrikų sąvoka darbuose nėra galutinai apibrėžta, jaučiamas mokslinių darbų, kuriuose siūloma naudoti agreguotas metrikas trūkumas.
4. Atliekamas tyrimas turėtų suteikti praktinę vertę informacijos saugos metrikų tyrimų srityje, o agreguotų metrikų naudojimas turėtų svariai prisidėti prie organizacijų informacijos saugos tobulinimo.

3. Agreguotų informacijos saugos metrikų sudarymo eigos aprašymas

Šiame skyriuje aprašoma tyrimo eiga – agreguotų metrikų sudarymo metodika. Skyrius susideda iš trijų poskyrių. Pirmajame poskyryje apibrėžiama agreguotos informacijos saugos metrikos sąvoka, pateikiamos siūloma metrikos skaičiavimo formulė bei aiškinamas pavyzdys. Antrajame skyriuje išskiriamos trijų ISO/IEC 27001 informacijos saugos standarto valdymo sričių klasikinės informacijos saugos metrikos. Trečiajame skyriuje aprašoma agreguotų informacijos saugos metrikų sudarymo metodika, kurios pagrindas daugiakriteriai metodai *AHP, WASPAS* ir *fuzzy TOPSIS*.

3.1. Agreguotų informacijos saugos metrikų apibūdinimas

Analitinės dalies skyriuje 2.1.2 pateikiamos klasikinės informacijos saugos metrikos. Jos susideda iš vieno dydžio arba vieno kintamojo. Kaip pavyzdys metrika – organizacijos serveriuose per dieną aptikto KPK skaičius, kuris matuojamas vienetais. Tai vieno kriterijaus metrika. Sudėjus bent dvi skirtingas metrikas ir įvertinus jų svarbą apibūdinančius svorio koeficientus galima gauti apibendrintą dydį – būtent tai vadiname agreguota informacijos saugos metrika. Šios agreguotos metrikos tikslas – nurodyti apibendrintą informacijos saugos padėtį organizacijoje. Kadangi kiekviena organizacija yra skirtinga, agreguotos informacijos saugos metrikos turėtų būti pritaikomos individualiai.

Toliau bus pateikiamas ir išaiškinamas agreguotos informacijos saugos metrikos pavyzdys. Tarkime, kad nagrinėjama sritis, kuri bus stebima taikant vieną agreguotą metriką, yra KPK poveikis organizacijoje. Nors šią agreguotą metriką galėtų sudaryti didelis kiekis skirtingų klasikinių metrikų, paprastumo dėlei bus naudojamos tik dvi klasikinės metrikos – KPK aptiktas organizacijos serveriuose ir KPK aptiktas darbuotojų kompiuteriuose. Natūralu, kad KPK, aptiktas viename iš organizacijos serverių, kels skirtingo tipo ir dydžio grėsmę informacijos saugos požiūriu, negu KPK aptiktas viename iš organizacijos darbuotojo kompiuterių. Šį grėsmės arba pažeidžiamumo santykį apibūdina svorio koeficientai, kurių nustatymas turėtų priklausyti nuo pačios organizacijos specifikos ar infrastruktūros, taip pat, jos tikslų ir poreikių. Pateiktame pavyzdyje, klasikinei metrikai „KPK aptiktas organizacijos serveriuose“ priskiriamas 70% svorio koeficientas. Kitai metrikai „KPK aptiktas darbuotojų kompiuteriuose“ suteikiamas 30% svorio koeficientas. Baigiamajame darbe svorio koeficientų gavimas bus atliekamas naudojantis daugiakriteriais sprendimų metodais. Kitas svarbus dydis įeinantis į agreguotos, metrikos apskaičiavimo formulę yra nuostatos vertė. Nuostatos vertės dydis formulėje turėtų būti nustatomas pagal konkrečią organizaciją ir apibūdinti toleruotiną įvykių skaičių, tai galėtų būti ir vidutinis įvykių skaičius per dieną ar kitą laiko matą. Šis dydis priklauso nuo organizacijos, jos dydžio ir veiklos pobūdžio. Tai dinaminis dydis, kuris laikui bėgant kinta ir turėtų būti nuolat peržiūrimas ir koreguojamas. Aptarto pavyzdžio apibūdinimas pateikiamas 8 lentelėje.

Turėdami klasikinių metrikų svorio koeficientus ir vidutinius įvykių skaičius galime apskaičiuoti agreguotą metriką. Tai atliekame pasiūlant formulę, kurią galima būtų naudoti skaičiuojant agreguotas metrikas:

$$f = \frac{\sum_{i=1}^{n}\left(\frac{a_i}{N_{a_i}} \cdot K_{a_i}\right)}{n} - \frac{1}{n} \qquad (1)$$

čia: f – agreguota informacijos saugos metrika; a_i – klasikinės metrikos įvykių skaičius realiu laiko momentu; N_{ai} – nuostatos vertė (nustatytas toleruotinas įvykių skaičius); K_{ai} – klasikinės metrikos svorio koeficientas; n – klasikinių metrikų sudarančių daugiakriterę, agreguotą, metriką skaičius. Reikia pažymėti, kad taikant šią formulę klasikinių metrikų svorio koeficientai privalo sudaryti 100 %, arba:

$$\sum_{i=1}^{n} K_{a_i} = 1 \qquad (2)$$

8 lentelė. Agreguotos informacijos saugos metrikos pavyzdžio parametrai

Agreguotos metrikos pavadinimas	**Klasikinės metrikos, kurios įeina į agreguotą metriką**	**Klasikinių metrikų svorio koeficientai agreguotoje metrikoje, %**	**Kintamasis, naudojamas metrikos apskaičiavimo formulėje**	**Agreguotos metrikos apskaičiavimo formulė**
KPK poveikis organizacijai	KPK aptiktas organizacijos serveriuose	70	a_1	$\frac{\frac{a_1}{N_{a_1}} \cdot 0{,}7 + \frac{a_2}{N_{a_2}} \cdot 0{,}3}{2} - \frac{1}{2}$; $N_{a1,a2}$ – nuostatos vertė (įvykių skaičius per dieną);
	KPK aptiktas darbuotojų kompiuteriuose	30	a_2	

Naudojantis šia formule apskaičiuojama apibendrintos daugiakriterės, agreguotos, informacijos saugos metrikos reikšmė. Galimi trys verčių intervalai, kurie atskleidžia skirtingas metrikos reikšmes. Reikšmė lygią 0, teigia, kad matuojamų dydžių vertės atitinka numatytoms (vidutinėms) normoms, kitaip sakant padėtis yra įprasta. Gavus reikšmę mažesnę negu 0, galima teigti, kad padėtis yra gerėjanti, numatytieji rodikliai nepasiekti. Idealiu atveju agreguota metrika turėtų būti lygi (-1)/n, tai reikštų, kad jokie neigiami įvykiai susiję su matuojamų metrikų sauga nevyksta. Gavus reikšmę didesnę negu 0 turime sutrikimų, rodikliai indikuoja apie informacijos saugos problemas. Rezultatų reikšmės ir apibūdinimai pateikiami 9 lentelėje:

9 lentelė. Agreguotos informacijos saugos metrikos formulės verčių apibūdinimas

Vertės intervalas	**Apibūdinimas**
=0	Organizacijos informacijos saugos padėtis yra įprasta, su sauga susijusių įvykių skaičius lygus organizacijos nustatytam vidurkiui.

Vertės intervalas	Apibūdinimas
>0	Organizacijos informacijos saugos padėtis yra neigiama Kuo šis dydis yra didesnis, tuo daugiau neigiamų įvykių turime.
<0	Organizacijos informacijos saugos padėtis yra teigiama. Kuo šis dydis yra artimesnis (-1)/n, tuo mažiau neigiamų įvykių turime. Idealiu atveju dydis lygus (-1)/n, kas reiškia, kad jokie neigiami informacijos saugos stebėsenos įvykiai nevyksta.

Baigiamojo darbo tikslas pasiūlyti apibendrintą informacijos saugos metrikų sąvoką pagrindinėms informacijos saugos valdymo sritims.

3.2. Klasikinės informacijos saugos metrikos, skirtos agreguotoms metrikoms sudaryti

Pagal šiuo metu taikomą tarptautinį informacijos saugos valdymo sistemos standartą ISO/IEC 27001 informacijos saugos metrikos yra privalomos (Azuwa et al., 2015). Standarte išskiriama 14 informacijos saugos valdymo sričių (ISO/IEC, 2013):

1) Informacijos saugos politikos – siekiama užtikrinti, kad būtų laikomasi informacijos saugos politikų;

2) Informacijos saugos organizaciniai aspektai – apima specifinių užduočių atlikimo tvarką ir atsakomybių pasiskirstymą;

3) Žmogiškųjų išteklių saugos – tikslas užtikrinti darbuotojų atsakomybes ir jų vykdymą;

4) Vertybių valdymo – apima informacijos ir informacinių vertybių apsaugą;

5) Prieigos kontrolės – tikslas užtikrinti, kad darbuotojai galėtų pasiekti tik informaciją susijusią su jų tiesioginėmis užduotimis. Didesnės prieigos teisės gali būti rimta grėsmė informacijos saugai;

6) Kriptografija – siekiama užtikrinti duomenų šifravimą ir saugų jautrios informacijos valdymą;

7) Fizinės saugos – apima organizacijos patalpų ir jose laikomos įrangos saugą;

8) Operacijų saugos – viena plačiausiu sričių apimanti: organizacijos veiklos operacijas, KPK, sistemų rezervinį kopijavimą, žurnalizavimą, programinės įrangos integralumo užtikrinimą, techninių pažeidžiamumų valdymą, informacinių sistemų auditavimą;

9) Komunikacijų saugos – apima informacijos apsaugą kompiuteriniuose tinkluose;

10) Sistemų įsigijimo, tobulinimo ir priežiūros – siekia užtikrinti informacijos saugos svarbą organizacijos informacinėse sistemose;

11) Tiekėjų santykių – apima organizacijos informacijos saugą susijusią su trečiosiomis šalimis, organizacijos partneriais;

12) Informacijos saugos incidentų valdymo – nusako darbuotojų atsakomybes ir veiksmų planą saugos incidento metu;

13) Informacijos saugos aspektai verslo tęstinumo valdymui – apima verslo sutrikimų valdymą, informacijos prieinamumo užtikrinimą;

14) Atitikimo standartams (angl. *compliance*) – užtikrina organizacijų gebėjimą laikytis įstatymų ir galiojančių informacijos saugos standartų atitikimą.

Visų šių sričių apimtyje vykstančių procesų efektyvumui matuoti taikomos informacijos saugos metrikos. Organizacijos specifika diktuoja, kokia metrikų programa turėtų būti naudojama. Darbe sudaromos agreguotos informacijos saugos metrikos trims ISO/IEC 27001 standarte apibrėžiamoms valdymo sritims: operacijų saugos, komunikacijų saugos ir sistemų įsigijimo, tobulinimo ir priežiūros. Pasirenkamos būtent šios, kadangi darbe stengiamasi orientuotis labiau į techninius saugumo aspektus. Pagal sritis bus atliekamas ir agreguotų, metrikų sudarymas. Tai atliksime išrenkant klasikines informacijos saugos metrikas, vėliau joms suteiksime svorio koeficientus.

Remiantis moksline literatūra ir verslo leidiniuose pateikiama informacija apie saugos metrikų rekomendacijas, kiekvienai iš pasirinktų informacijos saugos valdymo sričių išrenkamos klasikinės informacijos saugos metrikos. Iš šio sąrašo klasikinių metrikų bus siekiama išrinkti geriausias, kurios bus įtrauktos į agreguotą informacijos saugos metriką. Operacijų saugos srities klasikinės saugos metrikos pateikiamos 10 lentelėje, komunikacijų srities metrikos 11 lentelėje, o informacinių sistemų įsigijimo, tobulinimo ir priežiūros valdymo srities 12 lentelėje.

Operacijų saugos valdymo sričiai priskiriami tokie aspektai kaip (Irwin, 2020):

• Organizacijos veiklos operacijos – užtikrinimas, kad atsakingi asmenys tinkamai vykdytų procedūras;

• KPK - užtikrinimas, kad organizacija yra pasiruošusi ir žino apie galimas KPK grėsmes;

• Sistemų rezervinį kopijavimą – reikalavimai susiję su sistemų rezervinių kopijų atlikimu, siekiant išvengti duomenų praradimo;

• Žurnalizavimą ir monitoringą – leidžia turėti dokumentuotą įrodymą ir bazę saugos incidento tyrimui atlikti;

• Operacinių sistemų integralumo užtikrinimas – užtikrinimas, kad operacijas atliekanti programinė įranga yra integrali, tai atliekama kontroliuojant į OS įrašomą programinę įrangą;

• Techninių pažeidžiamumų valdymą – siekiama užtikrinti, kad neautorizuoti asmenys neišnaudotų sistemos pažeidžiamumų;

• Informacinių sistemų auditavimą – siekiama minimizuoti audito veiklos sutrikimus keliamus OS.

Tam, kad gautoje agreguotoje metrikoje būtų įvertinta dauguma operacijų saugos srities aspektų, atliekamas papildomas skirstymas į sritis. Iš kiekvienos srities ekspertiniu vertinimu bus atrenkamos geriausios

1-2 klasikinės metrikos. Operacijų saugai išskiriamos šios sritys: KPK ir OS integralumo, pažeidžiamumų valdymo, rezervinio kopijavimo, įvykių stebėjimo (angl. *monitoring*).

10 lentelė. Operacijų saugos srities klasikinės informacijos saugos metrikos, kurios bus naudojamos agreguotos metrikos sudarymui (Fasulo, 2019; Jaquith, 2007; Zhang, 2017)

Eil. Nr.	**Metrika**	**Apibūdinimas**
KPK ir OS integralumo užtikrinimas		
1.	Incidentai susiję su KPK (vnt.)	Parodo visų incidentų susijusių su KPK skaičių
2.	KPK aptiktas el. laiškų sistemoje (vnt.)	Parodo el. laiškų užterštumą KPK
3.	KPK aptiktas vartotojų lankomuose internetiniuose puslapiuose (vnt.)	Parodo darbuotojų polinkį lankytis KPK platinančiuose internetiniuose puslapiuose
4.	KPK failai aptikti organizacijos įrenginiuose (įeina visi organizacijos įrenginiai) (vnt.)	Signalizuoja apie organizacijos įrenginiuose aptinkamus KPK failus
5.	KPK failai aptikti organizacijos serveriuose (vnt.)	Signalizuoja apie organizacijos serveriuose aptinkamus KPK failus
6.	KPK failai aptikti organizacijos darbuotojų kompiuteriuose (vnt.)	Signalizuoja apie darbuotojų kompiuteriuose aptinkamus KPK failus
7.	KPK incidentai, reikalaujantys mechaniškai išvalyti sistemą (vnt.)	Parodo KPK incidentų keliamą grėsmę, taip pat kiek resursų yra skiriama KPK paveiktų sistemų valymui
Pažeidžiamumų valdymas		
8.	Pažeidžiamumus skenuojančia programine įranga nepadengiamos sistemos (vnt.)	Atskleidžia pažeidžiamumų skenavimo sistemos veikimo mastą
9.	Žinomų pažeidžiamumų skaičius (vnt.)	Parodo kiek pažeidžiamumų yra organizacijos informacinėse sistemose
10.	Laikas skiriamas pažeidžiamumo sutvarkymui (laikas)	Atskleidžia pažeidžiamumų kritiškumo lygį bei personalo pasiruošimą
11.	Randamų pažeidžiamumų skaičius per fiksuotą laiko vienetą (vnt.)	Atskleidžia pažeidžiamumų skenavimo sistemos efektyvumą bei bendrinį sistemų saugumą
Rezervinis kopijavimas		
12.	Rezervinio kopijavimo sistemos sutrikimų skaičius, įtraukiant duomenų kopijavimą ir atstatymą (vnt.)	Atskleidžia kaip dažnai patiriami rezervinio kopijavimo sistemos sutrikimai
13.	Rezervinio kopijavimo sistemos atsilikimas nuo nuostatos verčių, įtraukiant duomenų kopijavimą ir atstatymą (laikas)	Parodo, kiek vėluoja atliekamos duomenų kopijų atlikimas ir jų atstatymas
Įvykių stebėjimas (angl. *monitoring*)		
14.	Aktyviai nestebimos (angl. *monitored*) ar nežurnalizuojamos kritinės organizacijos sistemos (vnt.)	Atskleidžia įvykių stebėjimo sistemos efektyvumą bei kritinių sistemų stebėjimo mastą
15.	Reagavimo į žurnalinių įrašų ir monitoringo sistemų kritinius pranešimus laikas (laikas)	Atskleidžia personalo reagavimo į kritinius pranešimus greitį bei generuojamų pranešimų reikšmingumą

Komunikacijų saugos valdymo sričiai priskiriami tokie aspektai kaip (Irwin, 2020):

• Tinklo saugos valdymas, siekiama užtikrinti tinkluose esančios informacijos konfidencialumą, integralumą ir prieinamumą;

• Informacijos tranzitinės būsenos sauga.

Tam, kad gautoje agreguotoje metrikoje būtų įvertinta dauguma komunikacijų saugos srities aspektų, atliekamas papildomas skirstymas į sritis. Iš kiekvienos srities ekspertiniu vertinimu bus atrenkamos geriausios 1-2 klasikinės metrikos. Komunikacijų saugai išskiriamos šios sritys: el. laiškų sistema, ugniasienės valdymas, sesijų ir srauto stebėjimas, tinklo atakos.

11 lentelė. Komunikacijų saugos srities klasikinės informacijos saugos metrikos, kurios bus naudojamos agreguotos metrikos sudarymui (Fasulo, 2019; Jaquith, 2007; Zhang, 2017)

Eil. Nr.	**Metrika, mato vnt.**	**Apibūdinimas**
	El. laiškų sistema	
1.	Ateinančių el. laiškų skaičius (vnt.)	Įprasto el. laiškų srauto stebėjimas
2.	Aptikto šlamšto (angl. spam) kiekis (vnt.)	Atskleidžia el. laiškų filtravimo sistemos darbo efektyvumą
3.	Neaptikto šlamšto (angl. spam) kiekis (vnt.)	Parodo el. laiškų filtravimo sistemos efektyvumą klaidų skaičių
	Ugniasienės valdymas	
4.	Ugniasienės taisyklių pakeitimai (vnt.)	Parodo kaip dažnai yra keičiamos, kuriamos ir trinamos ugniasienės taisyklės
5.	Ugniasienės eksploatavimui reikalingi darbo ištekliai (praleistas laikas val.)	Parodo, kiek laiko yra skiriama ugniasienės nustatymams atlikti
	Sesijų ir srauto stebėjimas	
6.	Prisijungimai (sesijos) prie organizacijos internetu pasiekiamų serverių ir paslaugų (vnt.)	Parodo įprastą prisijungimų prie organizacijos teikiamų paslaugų skaičių ir leidžia daryti išvadas srautui išaugus
7.	Organizacijos tinklo srautas (B)	Parodo, koks yra vidutinis organizacijos tinklo srautas ir leidžia daryti išvadas srautui išaugus
8.	Įrenginių esančių įmonės vidiniame tinkle skaičius (vnt.)	Atskleidžia apie galimą grėsmę, naujai atsiradę įrenginiai gali būti naudojami atakos tikslais
	Tinklo atakos (Ugniasienės, IPS, IDS sistemų taisyklių suveikimai)	
9.	Tinklo atakų skaičius (įtraukiamos sėkmingos ir nesėkmingos) (vnt.)	Parodo kaip dažnai organizacija susiduria su sėkmingomis ir nesėkmingomis įsilaužimo atakomis
10.	Sėkmingų tinklo atakų skaičius (vnt.)	Parodo kaip dažnai organizacija susiduria su sėkmingomis atakomis
11.	Tinklo atakos MTTD (*mean time to detect*) (laikas)	Parodo kaip greitai pavyksta pastebėti įvykusią ataką prieš organizacijos kompiuterinį tinklą

Eil. Nr.	Metrika, mato vnt.	Apibūdinimas
12.	Tinklo atakos MTTR (*mean time to repair*) (laikas)	Parodo kaip greitai pavyksta ištaisyti įvykusios atakos padarinius`
13.	Organizacijos tinklo įrenginių skenavimo iš išorės incidentų skaičius (vnt.)	Atskleidžia apie organizacijos tinklo įrenginių skenavimo mastus, gali prognozuoti būsimų tinklo atakų skaičių

Sistemų įsigijimo, tobulinimo ir priežiūros saugos valdymo sritis rūpinasi tiek vidinių organizacijos informacinių sistemų tiek internete esančių paslaugų saugumu (Irwin, 2020).

Tam, kad gautoje agreguotoje metrikoje būtų įvertinta dauguma sistemų įsigijimo, tobulinimo ir priežiūros saugos srities aspektų, atliekamas papildomas skirstymas į sritis. Iš kiekvienos srities ekspertiniu vertinimu bus atrenkamos geriausios 1-2 klasikinės metrikos Informacinių sistemų įsigijimo, tobulinimo ir priežiūros saugai išskiriamos šios sritys: sistemų konfigūracijos, sistemų veiklos sutrikimų, antivirusinės programinės įrangos valdymas, kritinių atnaujinimų valdymas.

12 lentelė. Informacinių sistemų įsigijimo, tobulinimo ir priežiūros srities klasikinės informacijos saugos metrikos, kurios bus naudojamos agreguotos metrikos sudarymui (Fasulo, 2019; Jaquith, 2007; Zhang, 2017)

Eil. Nr.	Metrika	Apibūdinimas
Sistemų konfigūracija		
1.	Sistemų neatitinkančių apibrėžtos konfigūracijos skaičius (vnt.)	Atskleidžia sistemų konfigūravimo efektyvumą
2.	Sistemų konfigūracijos pakeitimų skaičius (vnt.)	Atskleidžia sistemų konfigūracijų pakitimų dažnį
3.	Sistemoms nepritaikytų konfigūracijos saugos griežtinimo (angl. *security hardening*) nustatymų skaičius (vnt.)	Atskleidžia konfigūracijos nustatymų griežtinimo taikymo mastą
Sistemų veiklos sutrikimai		
4.	Sistemų neveikimo laikas, į kurį įeina planuotas ir neplanuotas sistemų neveikimas (laikas)	Atskleidžia sistemų veikimo ir neveikimo santykį taip pat patikimumą
5.	Neplanuotas sistemų veiklos sutrikimas, dėl gedimų bei veiklos sutrikimų (laikas)	Atskleidžia kiek sistema gali tinkamai funkcionuoti be sutrikimų
6.	Sistemų MTBF (angl. *mean time between failures*) (Atskleidžia sistemų patikimumą) (laikas)	Atskleidžia sistemų patikimumą
7.	Sistemų MTTR (angl. *mean time to repair*) (laikas)	Atskleidžia sistemų gedimų reikšmingumą bei personalo gebėjimą šalinti gedimus
Sistemų antivirusinės programinės įrangos valdymas		
8.	Kompiuterinės darbo vietos ir serveriai neturintys veikiančios antivirusinės programinės įrangos (vnt.)	Atskleidžia neapsaugotų antivirusine programine įranga darbo vietų ir serverių skaičių (įranga gali būti neįrašyta arba išjungta)

Eil. Nr.	Metrika	Apibūdinimas
9.	Kompiuterinės darbo vietos ir serveriai neturintys naujausių antivirusinės programinės įrangos KPK duomenų bazės sąrašų (vnt.)	Atskleidžia antivirusinės programinės įrangos atnaujinimų taikymo efektyvumą, pasiruošimą KPK grėsmėms
Kritinių atnaujinimų valdymas		
10.	Sistemos negavusios kritinių programinės įrangos atnaujinimų (vnt.)	Atskleidžia kritinių atnaujinimų diegimo efektyvumą
11.	Laikas reikalingas kritiniams atnaujinimams įdiegti (laikas)	Atskleidžia kritinių atnaujinimų diegimo greitį
12.	Vėlavimas atlikti kritinį saugumo atnaujinimą (laikas)	Atskleidžia kritinių atnaujinimų diegimo atsilikimą nuo numatyto grafiko
13.	Kritiniams atnaujinimams ištestuoti skiriamas laikas (val.)	Atskleidžia, kiek laiko yra skiriama kritinių atnaujinimų išbandymui

3.3. MCDM metodų taikymas agreguotai informacijos saugos metrikai sudaryti

Šiame skyriuje aprašomas skirtingų MCDM metodų pritaikymas pagrindiniai baigiamojo darbo užduočiai pasiekti – agreguotoms informacijos saugos metrikoms sudaryti. Toliau aprašomi trys MCDM metodai: AHP, WASPAS ir Fuzzy TOPSIS. Kadangi sprendžiant agreguotų informacijos saugos metrikų sudarymo užduotį tenka naudoti vien tik kokybinius dydžius, reikalinga pasirinkti tinkamą tyrimo metodiką. Dėl šios priežasties bus naudojami du atskiri problemos sprendimo būdai:

1) Kriterijų svoriams nustatyti bus naudojamas AHP metodas, vėliau šie svoriai bus taikomi skaičiuojant WASPAS metodu.

2) Skaičiavimai ir svoriai nustatomi taikant Fuzzy TOPSIS metodą.

3.3.1. MCDM taikymo aprašymas

3.2 skyriuje pateikiamos klasikinės informacijos saugos metrikos, skirtos agreguotų daugiakriterių metrikų sudarymui. Norint pasiekti pagrindinį darbo tikslą, pasiūlyti agreguotas informacijos saugos metrikas, būtina iš pateiktų ISO/IEC 27001 standarto sričių, klasikinių saugos metrikų išrinkti geriausias bei suteikti joms svorio koeficientus. Tam bus taikomi daugiakriteriai sprendimų priėmimo metodai, kur naudojamas ekspertinis vertinimas.

Daugiakriteriuose sprendimų priėmimo metoduose labai svarbu teisingai pasirinkti vertinimo kriterijus. Analitinės dalies 2.1.1 skyriuje pateiktoje 2 lentelėje išskiriami skirtinguose moksliniuose straipsniuose nagrinėjami metrikos kokybės kriterijai. Tolesniam tyrimui pasirinkta naudoti kriterijus, kurie buvo apibrėžti viename iš mokslinių straipsnių, kalbančių apie informacijos saugos metrikų kokybę (Savola, 2013). Tyrimu siekta išsiaiškinti svarbiausius metrikos kokybės kriterijus ir jau buvo pritaikytas ekspertinis vertinimas (141

specialisto). Svarbiausi klasikinės metrikos kriterijai, kurie bus naudojami tyrime yra: korektiškumas (angl. *correctness*), galimybė išmatuoti (angl. *measurability*) ir reikšmingumas (angl. *meaningfulness*) (Savola, 2013).

Pagrindinis darbo tikslas gauti agreguotas informacijos saugos metrikas, kurias sudaro klasikinės informacijos saugos metrikos su atitinkamais svorio koeficientais. Neretai problemas sprendžiant naudojantis daugiakriteriais sprendimų priėmimo metodais stengiamasi taikyti bent du skirtingus sprendimo būdus. Tokio pačio principo laikomasi ir šiame darbe. Problemai spręsti bus taikomi du sprendimo būdai. Pirmiausiai taikant AHP metodą bus gaunami kriterijų svorio koeficientai, vėliau šie koeficientai bus taikomi atliekant skaičiavimus MCDM metodu *WASPAS*. Kitas problemos sprendimo būdas MCDM metodas *Fuzzy TOPSIS.*

Uždavinio sprendimas nepriklausomai nuo naudojamo MCDM metodo susideda iš šių žingsnių (Simanavičienė, 2013):

1. Pirmiausiai sudaromas nagrinėjamų alternatyvų, iš kurių išrenkamos racionalios alternatyvos vektorius:

$$A = (A_1, A_2, \dots, A_i, \dots, A_m) \tag{3}$$

Darbo 3.2 skyriuje trims ISO/IEC 27001 standarto informacijos saugos valdymo sritims buvo pasiūlyta 13–15 klasikinių saugos metrikų. Iš šių metrikų reikia išrinkti 4-5, kurios bus įtraukiamos į agreguotą informacijos saugos metriką. Šį vertinimą atlieka ekspertų grupė. Ekspertai turės pasirinkti, kuri kiekvienos srities metrika, jų manymu yra svarbiausia. Klausimynas pateikiamas darbo prieduose.

2.Antruoju žingsniu suformuojamas rodiklių, pagal kuriuos vertinamos alternatyvos, vektorius:

$$X = (X_1, X_2, \dots, X_j, \dots, X_n) \tag{4}$$

Svarbiausi klasikinės metrikos kriterijai, kurie bus naudojami ir šiame tyrime yra: korektiškumas (angl. *correctness*), galimybė išmatuoti (angl. *measurability*) ir reikšmingumas (angl. *meaningfulness*) (Savola, 2013).

3. Formuojama sprendimo priėmimo matrica $X_{[m \text{ x } n]}$, kurią sudaro *i*-osios alternatyvos kiekybiniai įverčiai pagal *j*-uosius rodiklius:

$$X_{[m\ x\ n]} = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ x_{m1} & x_{m2} & \dots & x_{mn} \end{pmatrix} \tag{5}$$

Kadangi nagrinėjamoje problemoje vyrauja kokybiniai kriterijai, bus taikomas ekspertinis vertinimas. Ekspertinis vertinimas atliekamas taikant lingvistinius terminus, kurie vėliau konvertuojami į skaitines vertes, remiantis 17 ir 18 lentelėmis.

4. Toliau taikomas *AHP* metodas kriterijų svorių nustatymui bei MCDM metodas *WASPAS*. Problemos sprendimo aprašymas taikant šiuos metodus aprašomas 3.3.2 ir 3.3.3 poskyriuose.

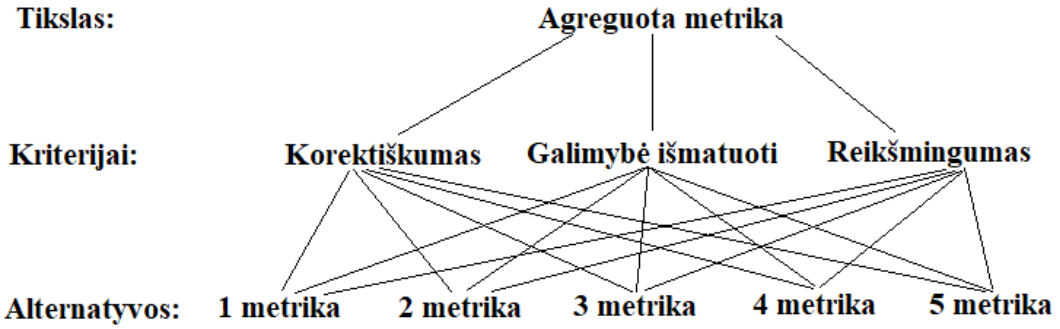
5. Problema sprendžiama *Fuzzy TOPSIS* metodu. Tolimesnis aprašymas pateikiamas 3.3.4 poskyryje.

Sprendžiamos MCDM problemos struktūrą apibrėžia 13 lentelė:

13 lentelė. Klasikinių informacijos saugos metrikų reitingavimo sprendimų matrica

	Kriterijai/Svoriai		
	Korektiškumas	**Galimybė išmatuoti**	**Reikšmingumas**
	S_1	**S_2**	**S_3**
Alternatyvos			
1 metrika	a_{11}	a_{12}	a_{13}
2 metrika	a_{21}	a_{22}	a_{23}
3 metrika	a_{31}	a_{32}	a_{33}
4 metrika	a_{41}	a_{42}	a_{43}
5 metrika	a_{51}	a_{52}	a_{53}

Sprendžiamą MCDM problemą paaiškina hierarchinė uždavinio struktūra:



1 pav. Agreguotų metrikų sudarymas taikant MCDM. Uždavinio hierarchinė struktūra

3.3.2. AHP taikymas kriterijų svorių nustatymui

Tik dalis MCDM metodų leidžia nustatyti kriterijų svorius. Vienas iš jų – metodas *AHP*. Jis leidžia išspręsti įvairaus pobūdžio problemas uždavinį išskaidant į hierarchinę struktūrą. *AHP* taikomas įvairaus tipo moksliniuose darbuose, pradedant tokiais kurių tikslas išsirinkti geriausią mobilųjį telefoną (Singh & Pattnaik, 2018) ir baigiant moksliniais darbais, kurie lygina kompanijose naudojamas informacijos saugos metrikas (Bhol et al., 2020). Pagrindiniai skaičiavimai bus atliekami kitu MCDM metodu *WASPAS*, kadangi *AHP* metodo struktūra tampa pernelyg kompleksiška esamos užduoties kontekste.

Kriterijų svorių nustatymo uždavinio sprendimas, taikant AHP metodą, susideda iš šių žingsnių (Simanavičienė, 2013):

1. Pirmuoju žingsniu suformuojamas rodiklių, pagal kuriuos vertinamos alternatyvos, vektorius:

$$X = (X_1, X_2, \dots, X_j, \dots, X_n) \quad (6)$$

Naudojami trys rodikliai: korektiškumas (angl. *correctness*), galimybė išmatuoti (angl. *measurability*) ir reikšmingumas (angl. *meaningfulness*) (Savola, 2013).

2. Įvedami rodiklių reikšmingumai, kuriuos nustato ekspertai. Ekspertų prašoma įvertinti trijų kokybinių kriterijų reikšmingumą metrikoje. Korektiškumo (angl. *correctness*), galimybės išmatuoti (angl. *measurability*) ir reikšmingumo (angl. *meaningfulness*) kriterijams suteikiant procentines vertes, pagal svarbą, apibrėžiančią metrikos kokybę. Tai atliekama taikant AHP metodo siūlomą kokybinių kriterijų vertinimo skalę ir sudarant palyginimo matricą (Poškas et al., 2012):

14 lentelė. Porinio palyginimo matrica

Kriterijai	**K_1**	**K_2**	**K_3**	**...**	**K_N**
K_1	1	pp_{12}	pp_{13}	...	pp_{1N}
K_2	pp_{21}	1	pp_{23}	...	pp_{2N}
K_3	pp_{31}	pp_{32}	1	...	pp_{3N}
...	...	...	...	...	...
K_N	pp_{N1}	pp_{N2}	pp_{N3}	...	1

Mūsų sprendžiamo uždavinio atveju ši lentelė atrodo taip:

15 lentelė. Kokybinių, metriką apibūdinančių, kriterijų porinio palyginimo matrica (Poškas et al., 2012)

Kriterijai	**Korektiškumas**	**Galimybė išmatuoti**	**Reikšmingumas**
Korektiškumas	1	pp_{12}	pp_{13}
Galimybė išmatuoti	pp_{21}	1	pp_{23}
Reikšmingumas	pp_{31}	pp_{32}	1

Taigi vertinimo uždavinį sprendžiantiems ekspertams reikės nustatyti porinio palyginimo koeficientų pp_{12}, pp_{13}, pp_{23} reikšmes. Reikšmės pp_{21}, pp_{31}, pp_{32} yra atvirkštinės, todėl yra apskaičiuojamos: $pp_{21}=1/pp_{12}$, $pp_{31}=1/pp_{13}$, $pp_{32}=1/pp_{23}$.

16 lentelė. AHP metodo kokybinių kriterijų porinio palyginimo skalė (Poškas et al., 2012; Saaty, 1987)

Vertinimas (reitingas)	**Vertinimo (reitingavimo) apibrėžimas**	**Vertinimo (reitingavimo) paaiškinimas**
1	Alternatyvų svarba lygi	Abi alternatyvos kriterijaus atžvilgiu yra vienodos
3	Silpnai pranašesnė viena už kitą	Eksperto nuomone, alternatyva yra silpnai pranašesnė už kitą
5	Svarbus pranašumas	Eksperto nuomone, alternatyva yra svarbiai pranašesnė už kitą
7	Labai svarbus pranašumas	Eksperto nuomone, alternatyva yra labai svarbiai pranašesnė už kitą
9	Absoliučiai svarbus pranašumas	Eksperto nuomone, alternatyva yra neginčijamai pranašesnė už kitą
2, 4, 6, 8	Tarpinės reikšmės	Kai reikalingas kompromisas
Vertinimas (reitingas)	**Vertinimo (reitingavimo) apibrėžimas**	
1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 1/9.	Atvirkštinis vertinimas. Jei *i* alternatyva buvo įvertinta alternatyvos *j* atžvilgiu, naudojant vieną iš aukščiau nurodytų skaičių *n*, priešinė alternatyvą *j* turės įvertinimą 1/*n*.	

Įverčiai pp_{12}, pp_{13}, pp_{21}, pp_{23}, pp_{31}, pp_{32} leidžia nustatyti šių kriterijų svorio koeficientus. Tai atliekama naudojant tam skirtą programinę įrangą. Darbe naudojama *SpiceLogic Analytic Hierarchy Process Software* bei *Excel* ruošiniai (Goepel, 2013). Gautos kriterijų svorių vertės naudojamos tolimesniuose skaičiavimuose, atliekamuose taikant metodą *WASPAS*.

3.3.3. WASPAS taikymo, agreguotai informacijos saugos metrikai sudaryti, aprašymas

Dar pakankamai naujas MCDM metodas *WASPAS* yra laikomas kaip pakankamai tikslus (Badalpur & Nurbakhsh, 2019). *WASPAS* metodas yra sudarytas iš dviejų metodų: *WSM* ir *WPM*.

WASPAS metodo pritaikymo žingsniai (Badalpur & Nurbakhsh, 2019; Chakraborty et al., 2015; Šilgalis, 2017):

1. Sudaroma sprendimų priėmimo matrica $x_{ij[m \times n]}$, kur x_{ij} yra vertė i – tosios alternatyvos j – tojo kriterijaus atžvilgiu, m yra alternatyvų skaičius ir n yra kriterijų skaičius. Kadangi vertinant informacijos saugos metrikas naudojami išimtinai tik kokybiniai kriterijai, reikalinga atlikti ekspertinį vertinimą. Ekspertiniam vertinimui bus taikomi lingvistiniai apibūdinimai, kurie bus konvertuoti į skaitines vertes. Konvertavimas atliekama naudojantis 17 lentele. Kriterijų svoriai gaunami, pagal praeitame skyriuje aprašytą metodiką (naudojantis *AHP* metodu).

17 lentelė. Ekspertų lingvistinių apibūdinimų konvertavimas į skaitines vertes (Badalpur & Nurbakhsh, 2019)

Lingvistinis terminas	**Kriterijaus skaitinė vertė (max)**	**Kriterijaus skaitinė vertė (min)**
Labai žemas (LŽ)	0	9
Žemas (Ž)	1	7
Vidutiniškas žemas (VŽ)	2	5
Vidutiniškas (V)	3	3
Vidutiniškas aukštas (VA)	5	2
Aukštas (A)	7	1
Labai aukštas (LA)	9	0

2. Atliekama normalizacija taikant formules:

Naudingam kriterijui:

$$\overrightarrow{x_{ij}} = \frac{x_{ij}}{max_{ij}\, x_{ij}} \tag{7}$$

Nenaudingam kriterijui:

$$\overrightarrow{x_{ij}} = \frac{min_{ij}\, x_{ij}}{x_{ij}}, \tag{8}$$

čia: $\overrightarrow{x_{ij}}$ yra normalizuota x_{ij} vertė.

2. Skaičiuojamas i – tosios alternatyvos optimalumo kriterijus (formulė pagrįsta *WSM* metodu):

$$Q_i^{(1)} = \sum_{j=1}^{n} \overrightarrow{X_{ij}}\, w_j, \tag{9}$$

čia w_j yra j – tojo kriterijaus svoris (nustatomas skyriuje 3.4 aprašyta metodika, taikant *AHP*).

3. Skaičiuojamas i – tosios alternatyvos optimalumo kriterijus (angl. *total relative importance*) (formulė pagrįsta *WPM* metodu):

$$Q_i^{(2)} = \prod_{j=1}^{n} \left(\overrightarrow{X_{ij}}\right)^{W_J}, \tag{10}$$

4. Sujungtas apibendrintas optimalumo kriterijus apskaičiuojamas taikant formulę:

$$Q_i = 0.5Q_i^{(1)} + 0.5Q_i^{(2)}. \tag{11}$$

5. Labiau apibendrinta lygtis optimalumo kriterijaus apskaičiavimui. Įvedamas dydis λ. Tai leidžia pasiekti aukštesnį reitingavimo tikslumą (Zavadskas et al., 2012):

$$Q_i = \lambda \sum_{j=1}^{n} \vec{X}_{ij} W_j + (1-\lambda) \prod_{j=1}^{n} \left(\vec{X}_{ij}\right)^{w_j},\ \lambda = 0, \dots, 1. \tag{12}$$

6. Optimalių λ verčių apskaičiavimas atliekamas taikant formulę:

$$\lambda = \frac{\sigma^2(Q_i^{(2)})}{\sigma^2\left(Q_i^{(1)}\right) + \sigma^2(Q_i^{(2)})}. \tag{13}$$

7. Dispersijų (angl. *variances*) $\sigma^2\left(Q_i^{(1)}\right)$ ir $\sigma^2\left(Q_i^{(2)}\right)$ apskaičiavimas atliekamas taikant formules:

$$\sigma^2\left(Q_i^{(1)}\right) = \sum_{j=1}^{n} W_j^2 \sigma^2(\vec{X}_{ij}) \vec{X}_{ij}, \tag{14}$$

$$\sigma^2\left(Q_i^{(2)}\right) = \sum_{j=1}^{n} \left(\frac{\prod_{j=1}^{n} \left(\overrightarrow{X_{ij}}\right)^{w_j} w_j}{\left(\overrightarrow{X_{ij}}\right)^{w_j} \left(\overrightarrow{X_{ij}}\right)^{(1-w_j)}} \right)^2 \sigma^2\left(\vec{X}_{ij}\right). \tag{15}$$

8. Alternatyvos išrikiuojamos prioritetine eilute, pagal jų naudingumo reikšmes. Iš šių reikšmių sudaroma agreguota informacijos saugos metrika (pagal 1 formulę). Gautos naudingumo reikšmės perskaičiuojamos į procentinę išraišką ir tampa svorio koeficientais. Tam naudojama formulė:

$$K_{a_i} = \frac{Q_i \cdot 100\%}{\sum_{i=1}^{n} Q_i}. \tag{16}$$

čia: K_{a_i} – klasikinės metrikos svorio koeficientas, agreguotoje metrikoje; Q_i – i - tosios alternatyvos optimalumo kriterijus; n – alternatyvų skaičius.

3.3.4. Fuzzy TOPSIS taikymo, agreguotai informacijos saugos metrikai sudaryti, aprašymas

TOPSIS metodas skirtas spręsti problemas apibrėžtoje aplinkoje, kai naudojami kiekybiniai dydžiai. Darbui neapibrėžtoje aplinkoje paprastai naudojamas, specialiai tam skirtas metodas *Fuzzy TOPSIS*. Užduoties sprendimas metodu *Fuzzy TOPSIS* atliekamas pagal šiuos žingsnius (Chen, 2000):

1. Sudaroma sprendimų priėmimo matrica $x_{ij[m x n]}$, kur x_{ij} yra vertė i – tosios alternatyvos j – tojo kriterijaus atžvilgiu, m yra alternatyvų skaičius ir n yra kriterijų skaičius. Kiekybinės vertės gaunamos taikant ekspertinį vertinimą. Ekspertų prašoma įvertinti tiek kokybės kriterijus tiek alternatyvas kiekvieno kriterijaus atžvilgiu taikant lingvistinius terminus. Lingvistiniai terminai konvertuojami į skaitines vertes, naudojantis 18 lentele:

18 lentelė. Lingvistinių verčių konvertavimas į skaitines taikant Fuzzy TOPSIS metodą (reitingams) (Chen, 2000)

Lingvistinis terminas	**Skaitinė vertė priskiriama kriterijams**	**Skaitinė vertė priskiriama alternatyvoms**
Labai žemas (LŽ)	(0, 0, 0.1)	(0, 0, 1)
Žemas (Ž)	(0, 0.1, 0.3)	(0, 1, 3)
Vidutiniškas žemas (VŽ)	(0.1, 0.3, 0.5)	(1, 3, 5)
Vidutiniškas (V)	(0.3, 0.5, 0.7)	(3, 5, 7)
Vidutiniškas aukštas (VA)	(0.5, 0.7, 0.9)	(5, 7, 9)
Aukštas (A)	(0.7, 0.9, 1.0)	(7, 9, 10)
Labai aukštas (LA)	(0.9, 1.0, 1.0)	(9, 10, 10)

2. Konstruojama normalizuota neraiškioji (angl. *fuzzy*) sprendimų priėmimų matrica:

$$R = [r_{ij}]_{m*n}, \quad i = 1,2,\dots,m; \quad j = 1,2,\dots,n. \tag{17}$$

Normalizuotos vertės naudingam ir nenaudingam kriterijui apskaičiuojamos taikant formules:

Naudingam kriterijui:

$$r_{ij} = \left(\frac{a_{ij}}{c_j^+}, \frac{b_{ij}}{c_j^+}, \frac{c_{ij}}{c_j^+}\right) \tag{18}$$

Nenaudingam kriterijui:

$$r_{ij} = \left(\frac{a_j^-}{c_{ij}}, \frac{a_j^-}{b_{ij}}, \frac{a_j^-}{a_{ij}}\right) \tag{19}$$

čia: c_j^+ - $max\{c_{ij}\}$ naudingajam kriterijui ir $a_j^- = min\{a_{ij}\}$ nenaudingam kriterijui.

3. Konstruojama pasverta normalizuota neraiškioji (angl. *fuzzy*) sprendimų priėmimų matrica:

$$V = [v_{ij}]_{m*n}, \quad i = 1,2,\dots,m; \quad j = 1,2,\dots,n \tag{20}$$

čia: $v_{ij} = r_{ij} \cdot w_j$ ir w_j yra j – tosios alternatyvos svoris.

4. Apibrėžiamos teigiamai idealaus (FPIS, A+) ir neigiamai idealaus (FNIS, A-) sprendimo apskaičiavimo formulės.

$$A^+ = (v_1^+, v_2^+, \dots, v_n^+) \tag{21}$$

$$A^- = (v_1^-, v_2^-, \dots, v_n^-) \tag{22}$$

Paprastai moksliniuose darbuose naudojami du idealaus sprendimo apibrėžimo būdai (Rejab et al., 2021):

1) Idealus sprendimas apibrėžiamas, kaip (Alidoosti et al., 2012):

Naudingam kriterijui: $A^+ = (1,1,1,\dots,1)$, A^-=(0,0,0,…,0); nenaudingam: $A^+ = (0,0,0,\dots,0)$, A^-=(1,1,1…,1).

2) Idealus sprendimas apibrėžiamas, kaip:

Naudingam kriterijui: $A^+ = (max_j v_{ij} | j = 1,2,\dots,m|)$, A^-=$(min_j v_{ij} | j = 1,2,\dots,m|)$.

Tolimesniuose skaičiavimuose bus naudojamas pirmasis variantas.

5. Skaičiuojamas atstumas tarp kiekvienos alternatyvos A^+ (d_i^+) ir A^- (d_i^-):

$$d_i^+ = \sum_{j=1}^{n} d(v_{ij}, v_j^+), \quad i = 1,2,\dots,m \tag{23}$$

$$d_i^- = \sum_{j=1}^{n} d(v_{ij}, v_j^-), \quad i = 1,2,\dots,m \tag{24}$$

6. Skaičiuojamas atstumas d (A,B):

$$d(A,B) = \sqrt{\frac{1}{3}((a_1 - a_2)^2 + (b_1 - b_2)^2 + (c_1 - c_2)^2)} \tag{25}$$

7. Skaičiuojamas kiekvienos alternatyvos artumo koeficientas (CC_i):

$$CC_i = \frac{d_i^-}{d_i^+ + d_i^-}, \quad i = 1,2,\dots,m \tag{26}$$

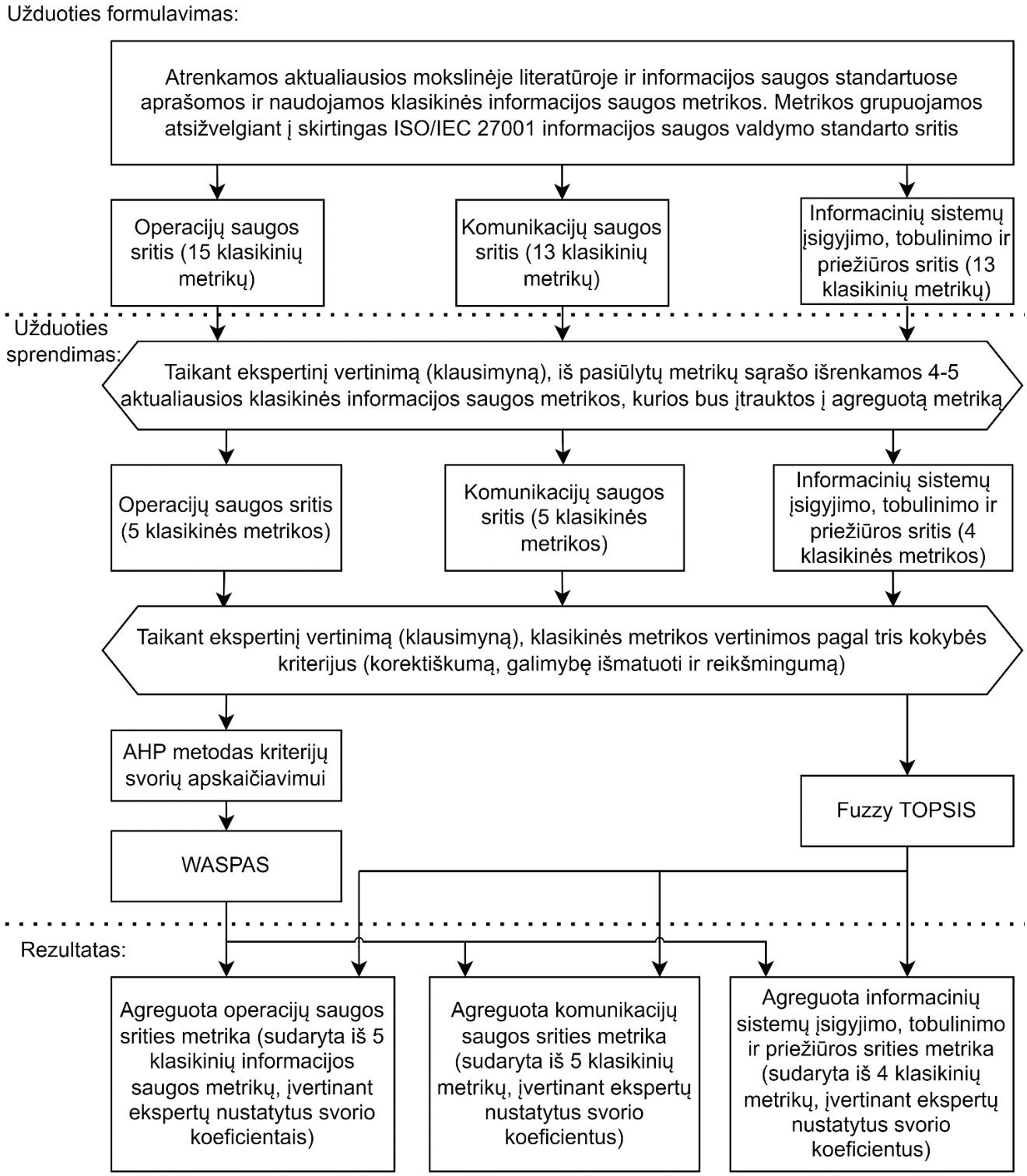
8. Alternatyvos reitinguojamos naudojantis gautomis artumo koeficiento CC_i vertėmis. Didžiausia artumo koeficiento vertė reiškia, kad alternatyva yra tinkamiausia.

9. Alternatyvos išrikiuojamos prioritetine eilute, pagal jų naudingumo reikšmes. Iš šių reikšmių sudaroma agreguota informacijos saugos metrika (pagal 1 formulę). Gautos naudingumo reikšmės perskaičiuojamos į procentinę išraišką ir tampa svorio koeficientais. Tam naudojama formulė:

$$K_{a_i} = \frac{CC_i \cdot 100\%}{\sum_{i=1}^{n} CC_i}. \tag{27}$$

čia: K_{a_i} – klasikinės metrikos svorio koeficientas, agreguotoje metrikoje; Q_i – i - tosios alternatyvos optimalumo kriterijus; n – alternatyvų skaičius.

Visą 3.4, 3.5 ir 3.6 skyriuje aprašytą MCDM metodų taikymo eigą apibūdina žemiau pateikiama problemos sprendimo metodikos diagrama:



2 pav. Užduoties sprendimo metodika

4. MCDM taikymas ir ekspertinis vertinimas agreguotoms informacijos saugos metrikoms sudaryti

Šiame skyriuje aprašomas 3 skyriuje minimų MCDM metodų taikymas agreguotoms informacijos saugos metrikoms sudaryti. Metodo pritaikymui naudojamas ekspertinis vertinimas. Skyriuje aprašoma ekspertinio vertinimo grupė, agreguotų metrikų sudarymas ir gautų rezultatų patikimumo patikrinimas.

4.1. Ekspertų grupė

Ekspertinio vertinimo tikslumas iš esmės priklauso, nuo vertinimą atliekančių ekspertų kompetencijos. Atliekant daugiakriterių uždavinių sprendimą, daugelis mokslininkų nurodo, kad optimaliausias grupės dydis yra nuo 8 iki 10 ekspertų. Kaip minimalus rekomenduotinas grupės dydis išskiriamas 3 ekspertų kiekis (NLP asociacija, 2014). Atliekamame tyrime ekspertų grupę iš viso sudaro 20 informacijos saugos srityje dirbantys arba mokslinę veiklą atliekantys specialistai. Pirmajame tyrimo etape dalyvauja 7 ekspertai, antrame kiti 10 ekspertų. Likę 3 ekspertai atliko metrikų verifikavimo dalį. Antrojo ir pirmojo etapo ekspertai yra skirtingi. Ekspertų vertinimams taikomi vienodi svoriai. Paprastai prieš atliekant problemos sprendimą taikant ekspertinį vertinimą, pirmiausiai atliekama ekspertų komandos atranka. Atrankos metu vertinama ekspertų kompetencija: pateikiamos anketos, taikomi savi vertinimo metodai ar kolektyvinis vertinimas (Ginevičius et al., 2009). Atliekant baigiamojo darbo tyrimą, ekspertų kompetencija nebuvo vertinama, kadangi nebuvo tokios galimybės. Ekspertų grupę sudarė informacijos saugos studijų programos, studentai ir šioje srityje dirbantys specialistai.

4.2. Agreguotų metrikų sudarymas

Ekspertinis vertinimas atliekamas pagal darbo 3.3 skyriuje aprašytą eigą. Kiekvienas ekspertas gauna vienodus klausimus, kurie pateikiami darbo priedų dalyje.

1. Ekspertams pateikiama užduotis atsakyti į 1 priedo klausimus ir tokiu būdu išrinkti aktualiausias 4 - 5 informacijos saugos metrikas, kurios bus įtraukiamos į agreguotą informacijos saugos metriką.

19 lentelė. Atsakymai į klausimyno klausimus (klasikinių informacijos saugos metrikų pasirinkimai)

	Klausimo numeris											
Ekspertas	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
E1	e), f)	c)	b)	a)	b)	a)	a)	b), d)	c)	b)	a)	a)
E2	a), d)	a)	a)	a)	c)	b)	b)	a), c)	c)	d)	b)	a)
E3	b), f)	d)	a)	b)	b)	a)	a)	a), e)	b)	b)	a)	a)
E4	a), f)	c)	a)	a)	c)	a)	b)	a), c)	a)	c)	a)	c)
E5	a), d)	c)	b)	b)	b)	a)	a)	c), d)	a)	d)	b)	a)
E6	a), e)	b)	a)	b)	c)	b)	a)	a), b)	c)	d)	b)	c)
E7	a), g)	b)	a)	b)	c)	a)	a)	a), c)	b)	d)	a)	a)

Remiantis 19 lentelėje pateiktais atsakymais į agreguotą metriką bus įtraukiamos šios klasikinės informacijos saugos metrikos:

Operacijų saugos sritis: 1. Incidentai susiję su KPK (vnt.); 2. KPK failai aptikti organizacijos darbuotojų kompiuteriuose (vnt.); 3. Laikas skiriamas pažeidžiamumo sutvarkymui (laikas); 4. Rezervinio kopijavimo sistemos sutrikimų skaičius, įtraukiant duomenų kopijavimą ir atstatymą (vnt.); 5. Reagavimo į žurnalinių įrašų ir monitoringo sistemų kritinius pranešimus laikas (laikas).

Komunikacijų saugos sritis: 1. Neaptikto šlamšto (angl. spam) kiekis (vnt.); 2. Ugniasienės taisyklių pakeitimai (vnt.); 3. Prisijungimai (sesijos) prie organizacijos internetu pasiekiamų serverių ir paslaugų (vnt.); 4. Tinklo atakų skaičius (įtraukiamos sėkmingos ir nesėkmingos) (vnt.); 5. Atakos MTTR (*mean time to repair*) (laikas).

Informacinių sistemų įsigijimo, tobulinimo ir priežiūros sritis: 1. Sistemoms nepritaikytų konfigūracijos saugos griežtinimo (angl. *security hardening*) nustatymų skaičius (vnt.); 2. Sistemų MTTR (*mean time to repair*) (laikas); 3. Kompiuterinės darbo vietos ir serveriai neturintys veikiančios antivirusinės programinės įrangos (vnt.); 4. Sistemos negavusios kritinių programinės įrangos atnaujinimų (vnt.).

Klasikinėms saugos metrikoms suteikiami šie simboliniai žymėjimai:

20 lentelė. Klasikinių saugos metrikų simboliniai žymėjimai

	Metrika	**Žymėjimas**
Operacijų sauga	1. Incidentai susiję su KPK (vnt.)	A_1
	2. KPK failai aptikti organizacijos darbuotojų kompiuteriuose (vnt.)	A_2
	3. Laikas skiriamas pažeidžiamumo sutvarkymui (laikas)	A_3
	4. Rezervinio kopijavimo sistemos sutrikimų skaičius, įtraukiant duomenų kopijavimą ir atstatymą (vnt.)	A_4
	5. Reagavimo į žurnalinių įrašų ir monitoringo sistemų kritinius pranešimus laikas (laikas)	A_5
Komunikacijų sauga	1. Neaptikto šlamšto (angl. spam) kiekis (vnt.)	A_1
	2. Ugniasienės taisyklių pakeitimai (vnt.)	A_2
	3. Prisijungimai (sesijos) prie organizacijos internetu pasiekiamų serverių ir paslaugų (vnt.)	A_3
	4. Tinklo atakų skaičius (įtraukiamos sėkmingos ir nesėkmingos) (vnt.)	A_4
	5. Atakos MTTR (*mean time to repair*) (laikas)	A_5
Sistemų sauga	1. Sistemoms nepritaikytų konfigūracijos saugos griežtinimo (angl. *security hardening*) nustatymų skaičius (vnt.)	A_1
	2. Sistemų MTTR (*mean time to repair*) (laikas)	A_2
	3. Kompiuterinės darbo vietos ir serveriai neturintys veikiančios antivirusinės programinės įrangos (vnt.)	A_3
	4. Sistemos negavusios kritinių programinės įrangos atnaujinimų (vnt.)	A_4

2. Antrajame tyrimo etape ekspertų prašoma įvertinti metriką apibūdinančius kriterijus, tam, kad nustatyti kriterijų svorio koeficientus (priedas nr. 2). Ekspertų šią užduotį prašoma atlikti du kartus, taikant *AHP* metodą bei *fuzzy TOPSIS*.

Kriterijų vertinimas *AHP* metodu

21 lentelė. AHP metodas. Ekspertų pateikti metrikos kokybės poriniai kriterijų vertinimai (kur, E – ekspertas nr. X, K – korektiškumas, G – galimybė išmatuoti, R – reikšmingumas, A – apibendrintas vertinimas)

E 1	**K**	**G**	**R**	**E 2**	**K**	**G**	**R**	**E 3**	**K**	**G**	**R**
K	1	5	1/8	**K**	1	8	1/7	**K**	1	5	1
G	1/5	1	1/9	**G**	1/8	1	1/8	**G**	1/5	1	1/7
R	8	9	1	**R**	7	8	1	**R**	1	7	1
E 4	**K**	**G**	**R**	**E 5**	**K**	**G**	**R**	**E 6**	**K**	**G**	**R**
K	1	5	1	**K**	1	9	7	**K**	1	3	1/2
G	1/5	1	1	**G**	1/9	1	1/8	**G**	1/3	1	1/2
R	1	1	1	**R**	1/7	8	1	**R**	2	2	1
E 7	**K**	**G**	**R**	**E 8**	**K**	**G**	**R**	**A**	**K**	**G**	**R**
K	1	3	1/2	**K**	1	7	1/8	**K**	1	5,24	0,5
G	1/3	1	1/4	**G**	1/7	1	1/8	**G**	0,19	1	0,21
R	2	4	1	**R**	8	8	1	**R**	2	4,75	1

Atliekame skaičiavimus naudodami tam specialiai skirtą programinę įrangą *SpiceLogic Analytic Hierarchy Process Software* bei *Excel* ruošinį (Goepel, 2013). Į klausimyną atsakė 10 ekspertų, tačiau 2 ekspertų pateiktus vertinimus pasirinkta atmesti, kadangi jų pateikti vertinimai buvo labai stipriai nesuderinti. Vertinimų atrinkimas atliekamas pagal suderinamumo reitingą (angl. *consistency ratio*). Naudojant *AHP* metodą teigiama, kad ekspertų pateiktų vertinimų suderinamumo reitingas neturėtų viršyti 10 % (Saaty, 1987). Turimu atveju apibendrintas suderinamumo reitingas buvo lygus 7,3 %, kas yra laikoma patenkinamu dydžiu, todėl vertinimą galima laikyti teisingu. Kitas dydis, kurį siūloma apskaičiuoti - konsensuso reitingas (angl. *consensus ratio*) turimu atveju yra lygus 75,4 %, kas reiškia, kad ekspertų sutarimas priimant šį sprendimą yra „aukštas“ (Goepel, 2013). Taigi apibendrinus visų ekspertų vertinimus gauname klasikinių informacijos saugos metrikų kokybės kriterijų svorio koeficientus:

Korektiškumas – 35,9 %; galimybė išmatuoti – 8,9 %, reikšmingumas – 55,2 %.

Kriterijų vertinimas *fuzzy TOPSIS* metodu

22 lentelė. Fuzzy TOPSIS metodas. Ekspertų pateikti kokybės kriterijų vertinimai (kur, E – ekspertas nr. X, K – korektiškumas, G – galimybė išmatuoti, R – reikšmingumas)

	Ekspertai									
Kriterijai	**E1**	**E2**	**E3**	**E4**	**E5**	**E6**	**E7**	**E8**	**E9**	**E10**
K	A	LA	LA	LA	A	A	LA	A	A	VA
G	V	A	V	VA	VA	LA	LA	VA	VA	VŽ
R	LA	LA	LA	A	LA	A	A	LA	LA	A

Šie ekspertų vertinimai bus naudojami tolimesniuose skaičiavimuose.

3. Trečiajame tyrimo etape ekspertai vertina atrinktas klasikines informacijos saugos metrikas pagal nurodytus kokybės kriterijus. Apklausa pateikiama priede nr. 3. Apklausos rezultatai pateikiami priede nr. 4.
4. Atliekami skaičiavimai WASPAS ir Fuzzy TOPSIS metodais.

WASPAS

Skaičiavimai atliekami naudojant (7-16) formules.

1. Sudaromos trys sprendimų priėmimo matricos, kuriose apskaičiuojami visų ekspertų pateiktų vertinimų vidurkiai:

23 lentelė. Sprendimų priėmimo matricos (WASPAS)

Operacijų sauga				**Komunikacijų sauga**				**Sistemų sauga**			
	K	**G**	**R**		**K**	**G**	**R**		**K**	**G**	**R**
A_1	5.3	6.2	5	A_1	3.8	3.7	3.9	A_1	5.6	6.1	6.8
A_2	5.7	6.7	5.7	A_2	5.2	6.5	4.9	A_2	6.3	6	7.6
A_3	5.9	5.3	4.8	A_3	5.8	6	4.9	A_3	6.8	8	6.6
A_4	5.4	4.4	4.9	A_4	5.5	6.2	7	A_4	6.6	7	7
A_5	6.3	6.9	6.8	A_5	5.5	6.2	6.6	A_5	-	-	-

2. Matricos normalizavimas atliekamas, pagal (7-8) formules:

24 lentelė. Normalizuotos sprendimų priėmimo matricos (WASPAS)

Operacijų sauga				**Komunikacijų sauga**				**Sistemų sauga**			
	K	**G**	**R**		**K**	**G**	**R**		**K**	**G**	**R**
A_1	0.84	0.90	0.74	A_1	0.66	0.57	0.56	A_1	0.82	0.76	0.89
A_2	0.91	0.97	0.84	A_2	0.90	1.00	0.70	A_2	0.93	0.75	1.00
A_3	0.94	0.77	0.71	A_3	1.00	0.92	0.70	A_3	1.00	1.00	0.87
A_4	0.86	0.64	0.72	A_4	0.95	0.95	1.00	A_4	0.97	0.88	0.92
A_5	1	1	1	A_5	0.95	0.95	0.94	A_5	-	-	-

3. Apskaičiuojamas pirmas optimalumo kriterijus naudojantis 9 formule:

25 lentelė. Pirmojo optimalumo kriterijaus vertės (WASPAS)

	A_1	**A_2**	**A_3**	**A_4**	**A_5**
Operacijų saugos $Q^{(1)}$	0.79	0.87	0.79	0.76	1
Komunikacijų saugos $Q^{(1)}$	0.59	0.80	0.83	0.98	0.95
Sistemų saugos $Q^{(1)}$	0.86	0.95	0.93	0.93	-

4. Apskaičiuojamas antras optimalumo kriterijus naudojantis 10 formule:

26 lentelė. Antrojo optimalumo kriterijaus vertės (WASPAS)

	A_1	**A_2**	**A_3**	**A_4**	**A_5**
Operacijų saugos $Q^{(2)}$	0.79	0.87	0.79	0.76	1
Komunikacijų saugos $Q^{(2)}$	0.59	0.79	0.82	0.98	0.95
Sistemų saugos $Q^{(2)}$	0.86	0.95	0.93	0.93	-

5. Skaičiuojamas bendras optimalumo kriterijus naudojantis 11 formule, taip pat naudojantis 16 formule gaunamas klasikinės metrikos svoris agreguotoje metrikoje:

27 lentelė. Bendrojo optimalumo kriterijaus vertės ir klasikinių metrikų svoriai agreguotoje metrikoje (WASPAS)

	Dydis	**A_1**	**A_2**	**A_3**	**A_4**	**A_5**
Operacijų sauga	$Q_{Bendras}$	0.79	0.87	0.79	0.76	1
	Rangas	4	2	3	5	1
	K_{ai}	18.68	20.74	18.78	18.06	23.75
Komunikacijų sauga	$Q_{Bendras}$	0.59	0.79	0.82	0.98	0.95
	Rangas	5	4	3	1	2
	K_{ai}	14.35	19.21	19.89	23.66	22.90
Sistemų sauga	$Q_{Bendras}$	0.86	0.95	0.93	0.94	-
	Rangas	4	1	3	2	-
	K_{ai}	23.36	25.90	25.26	25.48	-

Fuzzy TOPSIS

1. Sudaromos pradinės sprendimų priėmimo matricos:

28 lentelė. Sprendimų priėmimo matrica (Fuzzy TOPSIS)

	Operacijų sauga				**Komunikacijų sauga**				**Sistemų sauga**		
	K	**G**	**R**		**K**	**G**	**R**		**K**	**G**	**R**
A_1	[1,7,10]	[1,7.8,10]	[1,6.6,10]	A_1	[0,5.1,10]	[0,5.1,10]	[0,5.4,10]	A_1	[0,6.9,10]	[0,7.5,10]	[3,8.5,10]
A_2	[0,7.2,10]	[1,8.2,10]	[0,7.2,10]	A_2	[0,6.4,10]	[1,8.1,10]	[0,6,10]	A_2	[1,7.9,10]	[1,7.7,10]	[5,9.1,10]
A_3	[1,7.6,10]	[0,6.6,10]	[3,6.7,10]	A_3	[1,7.4,10]	[1,7.5,10]	[0,6.2,10]	A_3	[3,8.3,10]	[5,9.4,10]	[1,7.9,10]
A_4	[0,6.7,10]	[0,5.5,10]	[1,6.5,10]	A_4	[1,7.1,10]	[3,7.9,10]	[0,8.2,10]	A_4	[3,8.3,10]	[3,8.6,10]	[3,8.7,10]
A_5	[1,7.9,10]	[1,8.3,10]	[5,8.5,10]	A_5	[1,7.1,10]	[0,7.6,10]	[3,8.2,10]	A_5	-	-	-

2. Sprendimų priėmimo matricos normalizuojamos, naudojantis (18-19) formulėmis:

29 lentelė. Normalizuotos sprendimų priėmimo matricos (Fuzzy TOPSIS)

	Operacijų sauga			**Komunikacijų sauga**			**Sistemų sauga**		
	K	**G**	**R**	**K**	**G**	**R**	**K**	**G**	**R**
A_1	[0.1,0.7,1]	[0.1,0.78,1]	[0.1,0.66,1]	[0,0.51,1]	[0,0.51,1]	[0,0.54,1]	[0,0.69,1]	[0,0.75,1]	[0.3,0.85,1]
A_2	[0,0.72,1]	[0.1,0.82,1]	[0,0.72,1]	[0,0.64,1]	[0.1,0.81,1]	[0,0.6,1]	[0.1,0.79,1]	[0.1,0.77,1]	[0.5,0.91,1]
A_3	[0.1,0.76,1]	[0,0.66,1]	[0.3,0.67,1]	[0.1,0.74,1]	[0.1,0.75,1]	[0,0.62,1]	[0.3,0.83,1]	[0.5,0.94,1]	[0.1,0.79,1]
A_4	[0,0.67,1]	[0,0.55,1]	[0.1,0.65,1]	[0.1,0.71,1]	[0.3,0.79,1]	[0,0.82,1]	[0.3,0.83,1]	[0.3,0.86,1]	[0.3,0.87,1]
A_5	[0.1,0.79,1]	[0.1,0.83,1]	[0.5,0.85,1]	[0.1,0.71,1]	[0,0.76,1]	[0.3,0.82,1]	-	-	-

3. Svertinė normalizuota sprendimų priėmimo matrica, naudojama (20) formulė:

30 lentelė. Svertinės normalizuotos sprendimų priėmimo matricos (Fuzzy TOPSIS)

	Operacijų sauga			**Komunikacijų sauga**			**Sistemų sauga**		
	K	**G**	**R**	**K**	**G**	**R**	**K**	**G**	**R**
A_1	[0.05,0.644,1]	[0.01,0.546,1]	[0.07,0.634,1]	[0,0.469,1]	[0,0.357,1]	[0,0.518,1]	[0,0.635,1]	[0,0.525,1]	[0.21,0.816,1]
A_2	[0,0.663,1]	[0.01,0.574,1]	[0,0.691,1]	[0,0.588,1]	[0.01,0.567,1]	[0,0.576,1]	[0.050,0.727,1]	[0.01,0.539,1]	[0.35,0.874,1]
A_3	[0.05,0.699,1]	[0,0.462,1]	[0.21,0.643,1]	[0.05,0.680,1]	[0.01,0.525,1]	[0,0.595,1]	[0.15,0.761,1]	[0.05,0.658,1]	[0.070,0.758,1]
A_4	[0,0.616,1]	[0,0.385,1]	[0.07,0.624,1]	[0.05,0.653,1]	[0.03,0.553,1]	[0,0.787,1]	[0.15,0.764,1]	[0.03,0.602,1]	[0.21,0.835,1]
A_5	[0.05,0.727,1]	[0.01,0.581,1]	[0.35,0.816,1]	[0.05,0.653,1]	[0,0.532,1]	[0.21,0.787,1]	-	-	-

4. Skaičiuojamos teigiamai idealios (FPIS, $A+$) ir neigiamai idealios (FNIS, $A-$) alternatyvų vertės, pagal (21-22) formules:

31 lentelė. Teigiamai idealios (FPIS, A+) ir neigiamai idealios (FNIS, A-) alternatyvų vertės (Fuzzy TOPSIS)

	Dydis	**A_1**	**A_2**	**A_3**	**A_4**	**A_5**
Operacijų sauga, komunikacijų sauga, sistemų sauga	$A+$	1	1	1	1	1
	$A-$	0	0	0	0	0

5. Skaičiuojami santykiniai atstumai, atstumai iki idealios alternatyvos ir klasikinių metrikų svoriai agreguotoje metrikoje, pagal (23-27) formules:

32 lentelė. Santykiniai atstumai, atstumai iki idealios alternatyvos ir klasikinių metrikų svoriai agreguotoje metrikoje (Fuzzy TOPSIS)

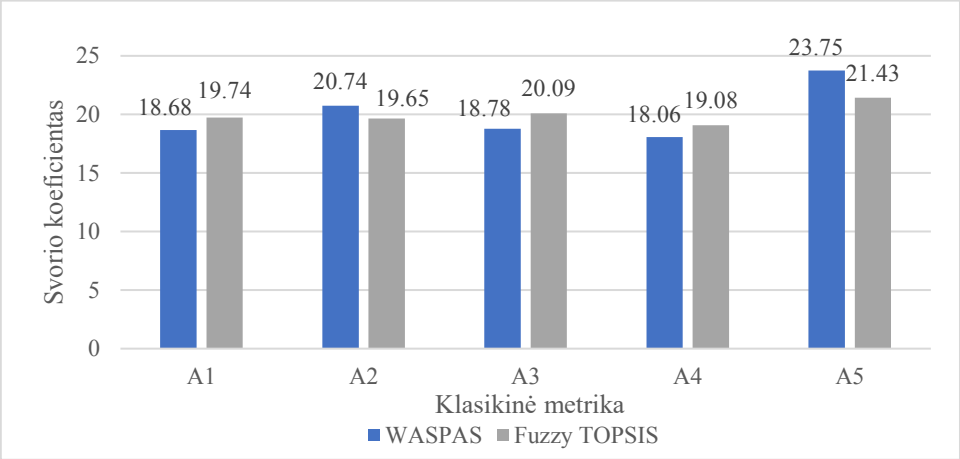
	Dydis	**A_1**	**A_2**	**A_3**	**A_4**	**A_5**
Operacijų sauga	d_i^+	1.79	1.84	1.73	1.88	1.58
	d_i^-	2.03	2.06	2.04	1.98	2.16
	CC_i	0.53	0.53	0.54	0.51	0.58
	K_{a_i}	19.74	19.65	20.09	19.08	21.43
Komunikacijų sauga	d_i^+	1.98	1.88	1.84	1.79	1.69
	d_i^-	1.90	2.00	2.02	2.08	2.09
	CC_i	0.49	0.52	0.52	0.54	0.55
	K_{a_i}	18.69	19.70	20.01	20.53	21.08
Sistemų sauga	d_i^+	1.72	1.58	1.65	1.58	-
	d_i^-	2.09	2.16	2.15	2.17	-
	CC_i	0.55	0.58	0.57	0.58	-
	K_{a_i}	24.16	25.43	24.94	25.47	-

Atlikus skaičiavimus WASPAS ir fuzzy TOPSIS metodais, gaunami metrikų svorio koeficientai. Skirtingais metodais gauti svorio koeficientai pateikiami 33 lentelėje:

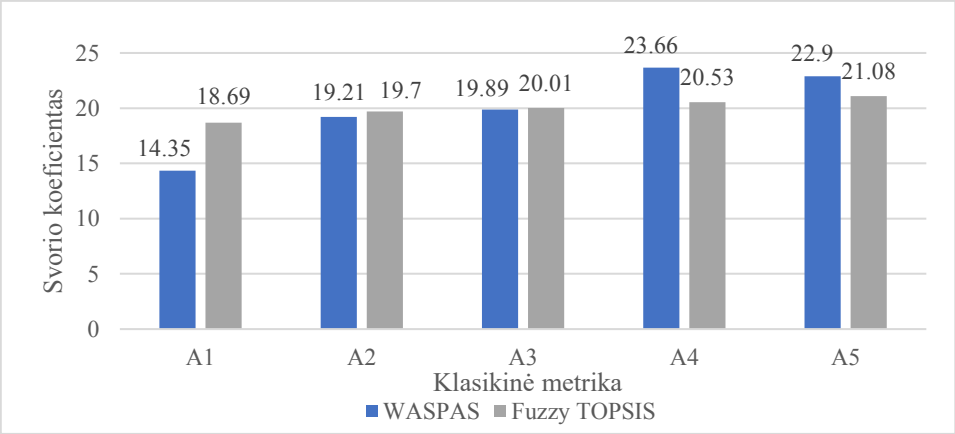
33 lentelė. Skirtingais problemos sprendimo būdais gautos klasikinių metrikų vertės agreguotoje metrikoje

Informacijos saugos valdymo sritys						
Klasikinė metrika	**Operacijų sauga**		**Komunikacijų sauga**		**Informacinių sistemų įsigijimo, tobulinimo ir priežiūros sauga**	
	Svorio koeficientas agreguotoje metrikoje		**Svorio koeficientas agreguotoje metrikoje**		**Svorio koeficientas agreguotoje metrikoje**	
	WASPAS	***Fuzzy* TOPSIS**	**WASPAS**	***Fuzzy* TOPSIS**	**WASPAS**	***Fuzzy* TOPSIS**
A1	18.68	19.74	14.35	18.69	23.36	24.16
A2	20.74	19.65	19.21	19.70	25.90	25.43
A3	18.78	20.09	19.89	20.01	25.26	24.94
A4	18.06	19.08	23.66	20.53	25.48	25.47
A5	23.75	21.43	22.90	21.08	-	-

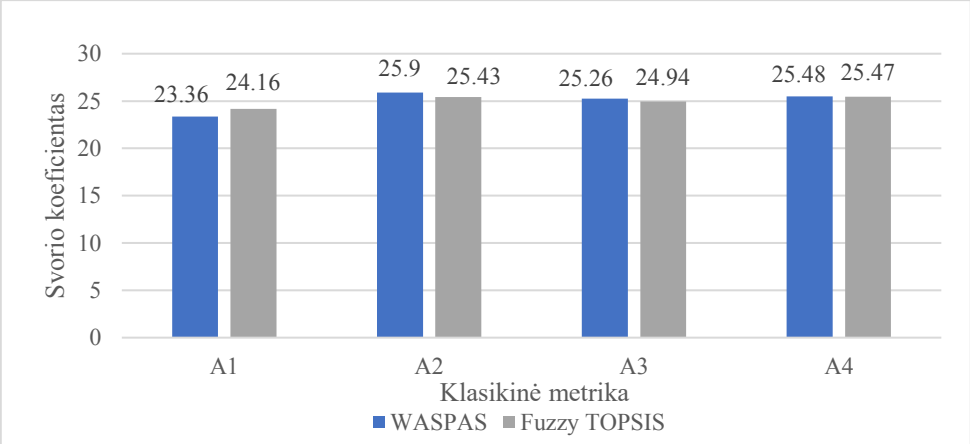
Pagal skirtingais problemos sprendimo būdais gautus rezultatus, braižomos stulpelinės diagramos, vaizduojančios klasikinių metrikų svorio koeficientus agreguotoje metrikoje:



3 pav. Operacijų saugos klasikinių metrikų svorio koeficientai agreguotoje metrikoje gauti skirtingais problemos sprendimo būdais



4 pav. Komunikacijų saugos klasikinių metrikų svorio koeficientai agreguotoje metrikoje gauti skirtingais problemos sprendimo būdais



5 pav. Informacinių sistemų įsigijimo, tobulinimo ir priežiūros saugos klasikinių metrikų svorio koeficientai agreguotoje metrikoje gauti skirtingais problemos sprendimo būdais

Dviem skirtingais problemos sprendimo būdais gautų klasikinių metrikų svorio koeficientų vertės buvo kiek skirtingos. Taip atsitiko dėl metodų *WASPAS* ir *fuzzy TOPSIS* skirtumų bei tam tikrų skaičiavimo ypatumų. Kokybės kriterijų svoriai (korektiškumas, galimybė išmatuoti ir reikšmingumas) skaičiuojant skirtingais metodais buvo skirtingi, taip pat buvo taikytas metodas *fuzzy* TOPSIS, kuris laikomas nelabai tinkamu kuomet turimi dideli skirtumai tarp alternatyvų vertinimų (Siksnelyte-Butkiene et al., 2020). Skaičiuojant metodu *fuzzy TOPSIS* galima naudoti du idealaus sprendinio variantus, šis pasirinkimas, gali stipriai nulemti galutinius atsakymus. Remiantis gautais metrikų koeficientais bei metodų patogumu prieita prie išvados, kad esamai užduočiai spręsti tinkamesnis yra *WASPAS* MCDM metodas.

Turint svorio koeficientus sudaromos trys agreguotų informacijos saugos metrikų apskaičiavimo formulės, kurias žymėsime simboliais $A_{operacijų}$, $A_{komunikacijų}$, $A_{sistemų}$. Naudojami svorio koeficientai apskaičiuoti metodu WASPAS. Formulės sudaromos pagal 3.1 skyriuje aprašytą metodiką (naudojant 1 formulę):

$$A_{operacijų} = \frac{\frac{a_1}{N_{a_1}}\cdot 0{,}187+\frac{a_2}{N_{a_2}}\cdot 0{,}207+\frac{a_3}{N_{a_3}}\cdot 0{,}188+\frac{a_4}{N_{a_4}}\cdot 0{,}181+\frac{a_5}{N_{a_5}}\cdot 0{,}238}{5} - \frac{1}{5}; \quad (28)$$

$$A_{komunikacijų} = \frac{\frac{b_1}{N_{b_1}}\cdot 0{,}144+\frac{b_2}{N_{b_2}}\cdot 0{,}192+\frac{b_3}{N_{b_3}}\cdot 0{,}199+\frac{b_4}{N_{b_4}}\cdot 0{,}237+\frac{b_5}{N_{b_5}}\cdot 0{,}229}{5} - \frac{1}{5}; \quad (29)$$

$$A_{sistemų} = \frac{\frac{c_1}{N_{c_1}}\cdot 0{,}234+\frac{c_2}{N_{c_2}}\cdot 0{,}259+\frac{c_3}{N_{c_3}}\cdot 0{,}253+\frac{c_4}{N_{c_4}}\cdot 0{,}255}{4} - \frac{1}{4}. \quad (30)$$

Dydžiai $N_{x_1}, N_{x_2}, N_{x_3}, N_{x_4}, N_{x_5}$ – atitinka organizacijos nustatytas vidutines metrikos vertes. Dydžiai a_1 – a_5, b_1 – b_5, c_1 – c_5 – atitinka klasikinės metrikos vertes (perskaičiuotas į procentinę išraišką). Vertės $N_{x_1}, N_{x_2}, N_{x_3}, N_{x_4}, N_{x_5}$ turi būti nuolatos peržiūrimos ir koreguojamos pagal esamą organizacijos padėtį.

Vertėtų pabrėžti, kad šios agreguotos metrikos apskaičiavimo formulės yra orientacinio pobūdžio, todėl taikant agreguotas metrikas praktikoje, galutinių verčių apskaičiavimo formulės turėtų būti pritaikytos pagal individualius poreikius.

Agreguotos metrikos gali suteikti galimybę efektyviau stebėti informacijos saugos padėtį organizacijoje, sudaryti apibendrintą vaizdą. Lyginant su klasikinėmis informacijos saugos metrikomis, agreguotos metrikos leidžia taupyti resursus, skiriamus informacijos saugos padėties stebėjimo procesui, taip pat duomenys gali pasitarnauti informuojant organizacijos vadovybę. Būtent organizacijos vadovybės informavimo pranašumai ir trūkumai, kuomet taikomos agreguotos informacijos saugos metrikos, bus tiriami baigiamojo darbo verifikavimo eksperimento skyriuje (5 skyrius).

4.3. Ekspertų nuomonių suderinamumo patikrinimas

Skyriuje aprašoma skaičiavimo metodika ir pateikiami skaičiavimų rezultatai, kuriais siekiama patikrinti ekspertų pateiktų kriterijų ir alternatyvų suderinamumą. Patikrinimas atliekamas skaičiuojant konkordancijos koeficientą, kuris apibūdina ar ekspertų nuomonės, dėl rodiklių reikšmingumų yra pakankamai suderintos (Simanavičienė, 2013). Konkordancijos koeficientas dar kitaip vadinamas Kendall‘o konkordancijos (*W*) koeficientu.

Kendall‘o konkordancijos koeficiento skaičiavimo eiga

Konkordancijos koeficientas skaičiuojamas remiantis šiais žingsniais (Andriušaitienė et al., 2008):

Pirmiausiai skaičiuojama kiekvienos alternatyvos įverčių suma:

$$R_i = \sum_{j=1}^{m} r_{i,j} \tag{31}$$

čia: R_i – alternatyvoms ekspertų suteiktų įverčių suma; m – ekspertų skaičius; $r_{i,j}$ – eksperto suteiktas alternatyvos i vertinimas.

Bendras vidurkis $\bar{R}$ skaičiuojamas pagal formulę:

$$\bar{R} = \frac{1}{n}\sum_{i=1}^{n} R_i \tag{32}$$

čia: n – alternatyvų skaičius.

Toliau skaičiuojama kvadratinių nuokrypių suma S:

$$S = \sum_{i=1}^{n}(R_i - \bar{R})^2 \tag{33}$$

Apskaičiuojamas Kendall‘o W koeficientas:

$$W = \frac{12 \cdot S}{m^2(n^3 - n)} \tag{34}$$

Kendall‘o konkordancijos koeficientas kinta rėžiuose tarp 0 ir 1. Vertė 0 reikštų visišką nesuderinamumą (kad ekspertų pateikti vertinimai atsitiktiniai), o 1 visišką suderinamumą (ekspertų pateikti vertinimai vienodi).

Tam, kad patvirtinti ekspertų pateiktų vertinimų suderinamumą, skaičiuojama konkordancijos koeficiento reikšmingumas:

$$\chi^2 = \frac{12 \cdot S}{m \cdot n \cdot (n+1)} \tag{35}$$

Apskaičiavus svarbos koeficientą χ^2 ši vertė lyginama su *chi* kvadrato skirsnio lentelės verte. Turint $v=n-1$ laisvės laipsnį randama kritinė reikšmė χ^2_{kr}. Pasirenkamas reikšmingumo lygis α. Rekomenduojamas ir dažniausiai pasitaikantis pasirinkimas 0,05 arba 0,01. Jei suskaičiuota χ^2 yra didesnė už χ^2_{kr} tada vertinimai laikomi suderintais (Andriušaitienė et al., 2008).

Kendall'o konkordancijos koeficiento skaičiavimai

Skaičiuojami konkordancijos koeficientai šioms ekspertų pateiktoms nuomonėms:

Fuzzy TOPSIS metodui skirtas metrikos kokybės kriterijų vertinimas:

$$W_1 = \frac{12 \cdot S}{m^2(n^3-n)} = \frac{12 \cdot 72}{10^2(3^3-3)} = 0{,}360 \quad (36)$$

Operacijų saugos metrikų vertinimas:

$$W_2 = \frac{12 \cdot S}{m^2(n^3-n)} = \frac{12 \cdot 5104}{10^2(15^3-15)} = 0{,}182 \quad (37)$$

Komunikacijų saugos metrikų vertinimas:

$$W_3 = \frac{12 \cdot S}{m^2(n^3-n)} = \frac{12 \cdot 7888}{10^2(15^3-15)} = 0{,}282 \quad (38)$$

Sistemų įsigijimo, priežiūros ir tobulinimo metrikų vertinimas:

$$W_4 = \frac{12 \cdot S}{m^2(n^3-n)} = \frac{12 \cdot 4394}{10^2(12^3-12)} = 0{,}307 \quad (39)$$

Bendras, visų atsakymų vertinimas (įtraukiant *Fuzzy* TOPSIS kriterijų, operacijų, komunikacijų, sistemų saugos alternatyvų vertinimus):

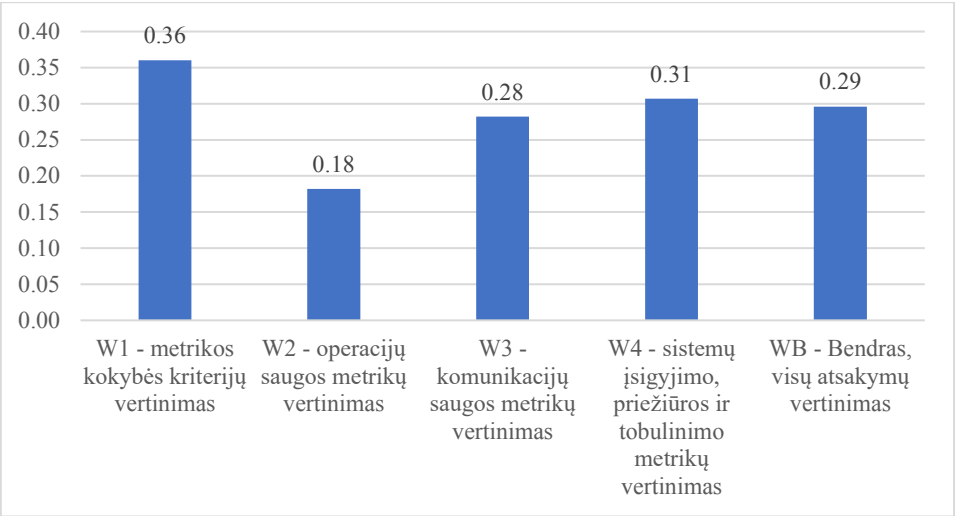
$$W_B = \frac{12 \cdot S}{m^2(n^3-n)} = \frac{12 \cdot 222840}{10^2(45^3-45)} = 0{,}294 \quad (40)$$

Toliau visoms ekspertų pateiktoms nuomonėms skaičiuojamos konkordancijos koeficiento reikšmingumo vertės (remiantis 35 formule). Gauti atsakymai pateikiami 34 lentelėje:

34 lentelė. Ekspertinio vertinimo suderinamumo skaičiavimai

	n	***W***	χ^2	χ^2_{kr}, (*ν=n-1*, α=0.05)	**Nuomonė laikoma suderinta (jei $\chi^2 > \chi^2_{kr}$)**
Fuzzy TOPSIS metodui skirtas metrikos kokybės kriterijų vertinimas	3	0,360	7,20	5,991	Taip
Operacijų saugos metrikų vertinimas	15	0,182	25,52	23,685	Taip
Komunikacijų saugos metrikų vertinimas	15	0,282	39,44	23,685	Taip
Sistemų įsigijimo, priežiūros ir tobulinimo metrikų vertinimas	12	0,307	33,80	19,675	Taip
Bendras, visų atsakymų vertinimas	45	0,294	129.18	60,481	Taip

Gautos vertės pateikiamos stulpelinėje diagramoje:



6 pav. Kendall'o *W* konkordancijos koeficientai apskaičiuoti skirtingoms ekspertinio vertinimo sritims

Apskaičiuotos konkordancijos koeficiento svarbos χ^2 vertės patvirtina, kad ekspertų nuomonės visais klausimais yra suderintos.

Gautos konkordancijos koeficiento *W* vertės turėtų būti interpretuojamos remiantis kiekvienos problemos specifika. Nėra nustatytų konkrečių rėžių, kurie teigtų, kad tam tikra koeficiento vertė yra tinkama ar ne. Šį koeficientą galima būtų pritaikyti tam tikrų ekspertų nuomonių atmetimui. Tai leistų gauti didesnį nuomonių suderinamumą, tačiau sprendžiant esamą problemą tokios praktikos nuspręsta nesilaikyti. Atliekant skaičiavimus pateiktus darbo 4 skyriuje buvo naudojami visi ekspertų atsakymai.

5. Verifikavimo eksperimentas

Šiame skyriuje aprašomas gautų agreguotų informacijos saugos metrikų verifikavimo eksperimentas. Verifikavimo eksperimento esmė – patikrinti agreguotų informacijos saugos metrikų efektyvumą jas naudojant praktikoje. Eksperimentu siekta palyginti klasikinių bei agreguotų metrikų privalumus ir trūkumus situacijoje, kuomet ruošiama mėnesinė informacijos saugos ataskaita.

Eksperimente simuliuojami du scenarijai:

1) Mėnesinės informacijos saugos ataskaitos ruošimas taikant vien tik klasikines informacijos saugos metrikas;

2) Mėnesinės informacijos saugos ataskaitos ruošimas taikant agreguotas informacijos saugos metrikas.

Mėnesinė informacijos saugos ataskaita bus pristatinėjama organizacijos vadovybei, juos ruošimu rūpinasi informacijos saugos specialistai. Esamu atveju šiai užduočiai atlikti bus naudojamas ekspertinis vertinimas.

Tyrime dalyvavo 3 ekspertai, kurie turėjo atlikti vienodas užduotis: paruošti informacijos saugos ataskaitas dviem nurodytais scenarijais. Vėliau ekspertų buvo paprašyta atsakyti į klausimyno klausimus. Toliau pateikiami pradiniai duomenys, kurie buvo suteikiami ataskaitos ruošimui:

		Mėnesio diena																													
Sritis	Klasikinė metrika	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Operacijų sauga	Incidentai susiję su KPK (vnt.)	6	4	4	6	3	5	7	1	8	5	1	8	10	6	10	4	4	2	0	9	6	4	0	1	10	2	2	1	4	7	10
	KPK failai aptikti organizacijos darbuotojų kompiuteriuose (vnt.)	7	1	1	8	0	4	3	5	7	3	5	7	3	8	6	7	7	1	6	8	7	4	4	8	5	5	7	1	6	7	6
	Laikas skiriamas pažeidžiamumo sutvarkymui (min)	95	18	51	31	25	220	68	157	18	131	233	199	206	21	129	266	5	231	50	120	226	199	48	298	272	289	173	49	152	217	298
	Rezervinio kopijavimo sistemos sutrikimų skaičius, įtraukiant duomenų kopijavimą ir atstatymą (vnt.)	8	8	1	7	10	4	10	8	10	2	5	2	7	8	10	7	0	3	5	9	2	2	1	7	0	6	2	7	4	10	5
	Reagavimo į žurnalinių įrašų ir monitoringo sistemų kritinius pranešimus laikas (min)	22	89	43	77	19	46	41	27	12	2	23	79	9	85	28	84	6	28	98	21	66	81	32	91	48	7	43	44	38	83	40
Komunikacijų sauga	Neaptikto šlamšto (angl. spam) kiekis (vnt.)	16	7	12	24	8	5	19	12	25	7	1	30	5	27	23	4	5	4	22	16	9	26	20	6	14	8	18	5	11	29	19
	Ugniasienės taisyklių pakeitimai (vnt.)	9	0	5	0	5	0	1	9	7	3	1	3	0	3	1	5	4	9	2	2	0	5	7	9	2	8	1	0	10	1	6
	Prisijungimai (sesijos) prie organizacijos internetu pasiekiamų serverių ir paslaugų (vnt.)	30527	87152	26548	47906	7729	87895	91555	57166	14372	52002	17818	49145	15081	73049	75929	60193	36241	89114	51982	11338	53523	30097	48105	47974	73406	38989	93159	94723	42865	33002	87848
	Tinklo atakų skaičius (įtraukiamos sėkmingos ir nesėkmingos) (vnt.)	18	28	17	16	1	4	8	2	7	15	9	24	5	6	23	18	5	15	21	2	2	19	29	10	27	10	4	8	19	22	19
	Atakos MTTR (Mean time to repair) (laikas)	13	36	170	118	35	32	48	10	27	90	65	120	99	20	184	68	198	5	76	100	49	136	146	168	139	48	5	6	21	64	1
Sistemų sauga	Sistemoms nepritaikytų konfigūracijos saugos griežtinimo (angl. security hardening) nustatymų skaičius (vnt.)	4	10	4	2	7	5	5	10	8	0	3	8	7	9	5	1	3	1	6	6	8	2	4	10	1	5	4	6	3	3	10
	Sistemų MTTR (Mean time to repair) (laikas)	5	0	4	8	1	6	7	7	8	5	7	6	8	7	4	0	6	6	3	6	0	3	5	3	7	8	5	4	4	1	8
	Kompiuterinės darbo vietos ir serveriai neturintys veikiančios antivirusinės programinės įrangos (vnt.)	299	50	98	103	273	30	129	281	17	31	290	294	263	107	204	240	163	250	132	252	152	68	106	268	223	272	261	61	126	254	299
	Sistemos negavusios kritinių programinės įrangos atnaujinimų (vnt.)	1	2	10	2	2	8	10	3	8	7	0	0	9	9	7	4	1	0	0	5	7	10	1	3	8	7	10	4	8	3	10

7 pav. Pradiniai verifikavimo eksperimento duomenys skirti ataskaitos ruošimui (klasikinių metrikų duomenys)

	Mėnesio diena																														
Agreguota metrika	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Operacijų saugos agreguota metrika	4.032	-10.4	-96.1	46.49	-84.5	2.87	5.121	-29.7	2.276	-87.6	-33.9	66.42	10.85	58.86	55.06	91.11	-104	-67.4	-2.57	47.43	44.38	13.07	-115	91.71	38.86	-21.8	-24.3	-79.2	-14.5	120.3	78.42
Komunikacijų saugos agreguota metrika	18.72	2.286	60.66	15.24	-102	-89.1	-23.5	-28	-25.8	-6.99	-102	88.4	-99.4	-25.5	110.2	10.35	18.24	23.03	26.25	-69.6	-104	78.05	141.4	78.87	86.44	-8.13	-65.1	-85.8	36.45	12.2	34.2
Sistemų saugos agreguota metrika	-21.4	-94.3	6.79	-60.7	-36.9	-4.15	68.6	91.53	51.71	-86.1	-21.9	22.92	139	93.8	17.98	-105	-67.2	-71.8	-96.1	47.68	-19.1	-39.6	-89.1	34.15	31.34	94.63	77.11	-58.1	-19.6	-76.5	198

8 pav. Pradiniai verifikavimo eksperimento duomenys skirti ataskaitos ruošimui (agreguotų metrikų duomenys)

Duomenys buvo generuojami naudojantis *Excel* funkcija *RANDBETWEEN* nurodant mažiausias bei didžiausias galimas vertes (taip, kad galima vertė būtų logiška).

Eksperimentu siekta išsiaiškinti pagrindinių ataskaitos ruošimo ir pristatymo kriterijų rezultatus:

1) Ataskaitos ruošimo laikas – atskleidžia, kiek laiko užtrunka paruošti ataskaitą;

2) Ataskaitos ruošimo patogumas – atskleidžia ar patogus ataskaitos ruošimas;

3) Rezultatų suprantamumas – atskleidžia, kiek gauti rezultatai yra lengvai suprantami. Reikėtų atsižvelgti ir į tai, kad rezultatai galimai bus pristatinėjami vadovybei, neturinčiai inžinerinio ar techninio išsilavinimo;

4) Rezultatų reikšmingumas – atskleidžia, kiek gauti rezultatai yra reikšmingi ir leidžiantys pasiremti priimant organizacijos informacijos saugos sprendimus;

5) Ataskaitos kokybė – atskleidžia kaip gerai paruošta ataskaita apibūdins organizacijos saugumo padėtį.

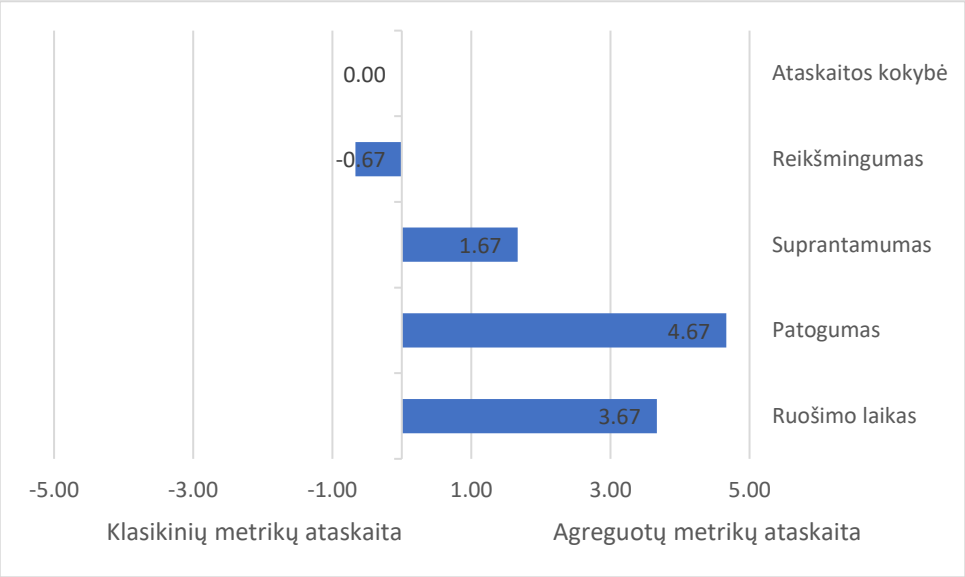
Remiantis šiais kriterijais buvo sudaryti klausimai, kuriais siekta palyginti ataskaitos ruošimo procesą naudojant klasikines bei agreguotas metrikas. Klausimai pateikiami 5 priede.

Toliau pateikiami ekspertų pateikti atsakymai į klausimyno klausimus:

35 lentelė. Ekspertų atsakymai į verifikavimo eksperimento klausimyną

	Klausimo numeris				
Ekspertas	**1**	**2**	**3**	**4**	**5**
E1	5	5	0	0	0
E2	2	5	5	0	0
E3	4	4	0	-2	0

Apskaičiuojami pateiktų atsakymų vidurkiai ir braižoma histograma:



9 pav. Agreguotų ir klasikinių metrikų taikymo palyginimo rezultatai

Pagal ekspertų pateiktus atsakymus galima teigti, kad agreguotų metrikų ataskaitos ruošimas yra patogesnis ir greitesnis taip pat pasiekiamas aukštesnis suprantamumas. Ataskaitos reikšmingumas šiek tiek nukenčia, o kokybė taikant agreguotas metrikas nepakinta.

6. Išvados

1. Išanalizavus literatūrą pastebėta, kad daugumoje mokslinių straipsnių siekiama informacijos saugos metrikas įvertinti, bet ne atlikti jų tobulinimą. Šio baigiamojo darbo tikslas – tobulinti informacijos saugos metrikas. Tikslui pasiekti buvo pasirinkta pasiūlyti agreguotas informacijos saugos metrikas, kurios būtų sudarytos iš klasikinių informacijos saugos metrikų, įtraukiant jų svarbą apibūdinančius svorio koeficientus.

2. Darbe buvo sudaryta metodika, leidžianti konstruoti agreguotas informacijos saugos metrikas. Agreguotų metrikų sudarymas buvo atliktas remiantis informacijos saugos valdymo standarto ISO/IEC 27001 sritimis. Sudarytoje metodikoje buvo taikomi 2 problemos sprendimo būdai. Remiantis gautais metrikų koeficientais bei metodų patogumu prieita prie išvados, kad esamai užduočiai spręsti tinkamesnis yra *WASPAS* MCDM metodas.

3. Pirmuoju tyrimo etapu buvo atrinkta 14 klasikinių informacijos saugos metrikų, skirtų agreguotų metrikų skaičiavimui. Šis tyrimo etapas, atskleidžia ekspertinės nuomonės išvadą – tinkamiausias 14 klasikinių metrikų. Antruoju tyrimo etapu buvo įvertintos prieš tai atrinktos, svarbiausios, 14 informacijos saugos metrikų pagal tris kokybės kriterijus: korektiškumą, galimybę išmatuoti ir reikšmingumą. Taikant 2 problemos sprendimo būdus, skirtingais MCDM metodais apskaičiuoti klasikinių metrikų svorio koeficientai ir pasiūlytos agreguotos metrikos. Dviem skirtingais problemos sprendimo būdais gautų klasikinių metrikų svorio koeficientų vertės buvo kiek skirtingos. Taip atsitiko dėl metodų *WASPAS* ir *fuzzy TOPSIS* skirtumų bei tam tikrų skaičiavimo ypatumų. Kokybės kriterijų svoriai (korektiškumas, galimybė išmatuoti ir reikšmingumas) skaičiuojant skirtingais metodais buvo skirtingi, taip pat buvo taikytas metodas *fuzzy* TOPSIS, kuris laikomas nelabai tinkamu kuomet turimi dideli skirtumai tarp alternatyvų vertinimų (Siksnelyte-Butkiene et al., 2020). Skaičiuojant metodu *fuzzy TOPSIS* galima naudoti du idealaus sprendimo variantus, šis pasirinkimas, gali stipriai nulemti galutinius atsakymus.

4. Siekiant patvirtinti pagrindinį darbo tikslą informacijos saugos metrikų tobulinimo užduoties įvykdymą, buvo atliekamas verifikavimo eksperimentas, kurio metu lygintos agreguotos ir klasikinės informacijos saugos metrikos. Eksperimentas parodė, kad agreguotų metrikų naudojimas gali būti patogesnis ir greitesnis procesas taip pat pasiekiamas aukštesnis suprantamumas. Rezultatų reikšmingumas šiek tiek nukenčia, o kokybė taikant agreguotas metrikas lyginant su klasikinėmis nepakinta.

7. Literatūra

Abbadi, Z. (2006). *Security Metrics. What Can We Measure ?* https://owasp.org/www-pdf-archive/Security_Metics-_What_can_we_measure-_Zed_Abbadi.pdf

Ahmed, R. K. A. (2016). Overview of Security Metrics. *Software Engineering*, *4*(4), 59–64. https://doi.org/10.11648/j.se.20160404.11

Ahmed, Y., Naqvi, S., & Josephs, M. (2018). Aggregation of security metrics for decision making: A reference architecture. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3241403.3241458

Alidoosti, A., Yazdani, M., Fouladgar, M. M., & Basiri, M. H. (2012). Risk assessment of critical asset using fuzzy inference system. *Risk Management*, *14*(1), 77–91. https://doi.org/10.1057/rm.2011.19

Andriušaitienė, D., Ginevičienė, V. B., & Šileika, A. (2008). Daugiakriterinis profesinio mokymo kokybės valdymo vertinimo modelis. *Verslas: Teorija Ir Praktika*, *9*(2), 88–96. https://doi.org/10.3846/1648-0627.2008.9.88-96

Azuwa, M. P., Ahmad, R., Sahib, S., & Shamsuddin, S. (2015). Technical Security Metrics Model in Compliance with ISO/IEC 27001 Standard. *International Journal of Cyber-Security and Digital Forensics*, *1*(4), 280–288.

Badalpur, M., & Nurbakhsh, E. (2019). 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

Bhol, S., Mohanty, J., & Pattnaik, P. (2020). *Cyber Security Metrics Evaluation Using Multi-criteria Decision-Making Approach* (pp. 665–675). https://doi.org/10.1007/978-981-32-9690-9_71

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. *Advances in Intelligent Systems and Computing*, *353*, 311–316. https://doi.org/10.1007/978-3-319-16486-1_31

Bodeau, D., Graubart, R., McQuaid, R., & Woodill, J. (2018). *Cyber Resiliency Metrics , Measures of Effectiveness , and Scoring*. https://www.mitre.org/sites/default/files/publications/pr-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf

Caballero, A. (2014). Information Security Essentials for IT Managers. *Managing Information Security*, 1–45. https://doi.org/10.1016/b978-0-12-416688-2.00001-5

Chakraborty, S., Zavadskas, E. K., & Antucheviciene, J. (2015). Applications of WASPAS method as a multi-criteria decision-making tool. *Economic Computation and Economic Cybernetics Studies and Research*, *49*(1), 1–17.

Chen, C.-T. (2000). A note on "extension of fuzzy TOPSIS method based on interval-valued fuzzy sets." *Applied Soft Computing Journal*, *26*, 513–514. https://doi.org/10.1016/j.asoc.2014.10.013

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008). *NIST Special Publication 800-55 Revision 1 easurement Guide for Information Security*. *July*.

Fasulo, P. (2019). *Top 20 Cybersecurity KPIs to Track in 2021*. https://securityscorecard.com/blog/9-cybersecurity-metrics-kpis-to-track

Ginevičius, R., Zubrecovas, V., & Tomas, G. (2009). Nekilnojamo turto investicinių projektų vertinimo metodikos. *Verslas: Teorija Ir Praktika*, *10*(3), 181–190.

Goepel, K. D. (2013). Implementing the Analytic Hierarchy Process as a Standard Method for Multi- Criteria Decision Making In Corporate Enterprises – A New AHP Excel Template with Multiple Inputs. *Proceedings of the International Symposium on the Analytic Hierarchy Process 2013*, 1–10.

Hallberg, J., Eriksson, M., Granlund, H., Kowalski, S., Lundholm, K., Monfelt, Y., Pilemalm, S., Wätterstam, T., & Yngström, L. (2011). Controlled Information Security Results and conclusions from the research project. *FOI, Swedish Defence Research Agency*, *March 2011*, 1–42.

Irwin, L. (2020). *ISO 27001: The 14 control sets of Annex A explained*. https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained

ISO/IEC. (2013). *"ISO/IEC 27001:2013E - Information technology -- Security techniques -- Information security management systems - Requirements." International Organization for Standardization.*

ISO/IEC. (2016). *"ISO/IEC 27004:2016E - Information technology -- Security techniques -- Information security management - Monitoring, measurement, analysis and evaluation." International Organization for Standardization*.

Jaquith, A. (2007). *Security Metrics: Replacing Fear, Uncertainty, and Doubt*.

Julisch, K. (2009). A Unifying Theory of Security Metrics with Applications with Applications. *Security*, 19. http://domino.watson.ibm.com/library/cyberdig.nsf/papers/223F8EBC4CC2C3AC852576F800426C0E/$File/rz3758.pdf

Kahraman, C., Öztayşi, B., Uçal Sari, I., & Turanoğlu, E. (2014). Fuzzy analytic hierarchy process with interval type-2 fuzzy sets. *Knowledge-Based Systems*, *59*, 48–57. https://doi.org/10.1016/j.knosys.2014.02.001

Kaur, M., & Jones, A. (2008). Security Metrics - A Critical Analysis of Current Methods. *Australian Information Warfare and Security Conference*, 41–47. https://doi.org/10.4225/75/57a8299daa0dd

Keršulienė, V., Zavadskas, E. K., & Turskis, Z. (2010). Selection of Rational Dispute Resolution Method By Applying New Step-Wise Weight Assessment Ratio Analysis (Swara). *Journal of Business Economics and Management*, *11*(2), 243–258. https://doi.org/10.3846/jbem.2010.12

Neto, A. A., & Vieira, M. (2011). Benchmarking Untrustworthiness. *International Journal of Dependable and Trustworthy Information Systems*, *1*(2), 32–54. https://doi.org/10.4018/jdtis.2010040102

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

Ouchani, S., & Debbabi, M. (2015). Specification, verification, and quantification of security in model-based systems. *Computing*, *97*(7), 691–711. https://doi.org/10.1007/s00607-015-0445-x

Pendleton, M., Garcia-Lebron, R., & Xu, S. (2016). A Survey on Security Metrics. *ACM Comput. Surv. 49, 4, Article 62*. https://doi.org/https://doi.org/10.1145/3005714

Peterson, E. (2006). The Big Book of Key Performance Indicators. *Web Analytics Demystified*.

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

Purboyo, T. W., Rahardjo, B., & Kuspriyanto. (2011). Security metrics: A brief survey. *Proceedings - International Conference on Instrumentation, Communication, Information Technology and Biomedical Engineering 2011, ICICI-BME 2011*, *March 2016*, 79–82. https://doi.org/10.1109/ICICI-BME.2011.6108598

Qadir, S., & Quadri, S. M. K. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security*, *07*(03), 185–194. https://doi.org/10.4236/jis.2016.73014

Ramos, A., Lazar, M., Filho, R. H., & Rodrigues, J. J. P. C. (2017). Model-Based Quantitative Network Security Metrics: A Survey. *IEEE Communications Surveys and Tutorials*, *19*(4), 2704–2734. https://doi.org/10.1109/COMST.2017.2745505

Rejab, E. N., Haridan, N. A., Nizam, N. E. N. S., & Rodzi, Z. M. (2021). The TOPSIS of Different Ideal Solution and Distance Formula of Fuzzy Soft Set in Multi-Criteria Decision Making. *International Journal of Academic Research in Economics and Management Sciences*, *10*(2), 87–91. https://doi.org/10.6007/ijarems/v10-i2/10063

Saaty, R. W. (1987). The analytic hierarchy process-what it is and how it is used. *Mathematical Modelling*, *9*(3–5), 161–176. https://doi.org/10.1016/0270-0255(87)90473-8

Savola, R. (2013). Quality of security metrics and measurements. *Computers & Security*, *37*, 78–90. https://doi.org/https://doi.org/10.1016/j.cose.2013.05.002

Savola, R. (2007). Towards a Security Metrics Taxonomy for the Information and Communication Technology Industry. *International Conference on Software Engineering Advances (ICSEA 2007)*, 60. https://doi.org/10.1109/ICSEA.2007.79

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*(Mcdm), 1164. https://www.mdpi.com/1996-1073/13/5/1164

Šilgalis, M. (2017). Jūrinių Vėjo Jėgainių Pamatų Tipų Analizė Ir Vertinimas Daugiatiksliais Vertinimo Metodais. *Klaipėdos Universitetas*.

Simanavičienė, R. (2011). Kiekybinių daugiatikslių sprendimo priėmimo metodų jautrumo analizė: daktaro disertacija. *Vilnius: Technika.*, 148. https://doi.org/10.20334/1973-m

Simanavičienė, R. (2013). Statistinių metodų taikymas daugiatikslių sprendimų patikimumui įvertinti. *Informacijos Mokslai*, *65*, 120–126. https://doi.org/10.15388/Im.2013.0.2048

Singh, S., & Pattnaik, P. K. (2018). Recommender System for Mobile Phone Selection. *International Journal of Computer Science and Mobile Applications*, *6*(4), 150–162.

Solana-González, P., Vanti, A. A., & Hackbart Souza Fontana, K. (2019). Multicriteria analysis of the compliance for the improvement of information security. *Journal of Information Systems and Technology Management*, *16*, 1–19. https://doi.org/10.4301/s1807-1775201916007

Stojić, G., Stević, Ž., Antuchevičiene, J., Pamučar, D., & Vasiljević, M. (2018). A novel rough WASPAS approach for supplier selection in a company manufacturing PVC carpentry products. *Information (Switzerland)*, *9*(5). https://doi.org/10.3390/info9050121

Tijink Gerwin, Kaveriappa, M., & Stack, S. (2019). *Next-gen Unified Security Metrics. Executive Summary*. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/next-gen-unified-security-metrics-white-paper.pdf

Velasquez, M., & Hester, P. (2013). An analysis of multi-criteria decision making methods. *International Journal of Operations Research*, *10*(2), 56–66.

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

Yasasin, E., & Schryen, G. (2015). Requirements for it security metrics - an argumentation theory based approach. *23rd European Conference on Information Systems, ECIS 2015*, *2015-May*, 0–16.

Yee, G. O. M. (2019). Designing good security metrics. *Proceedings - International Computer Software and Applications Conference*, *2*, 580–585. https://doi.org/10.1109/COMPSAC.2019.10270

Zavadskas, E. K., Turskis, Z., Antucheviciene, J., & Zakarevicius, A. (2012). Optimization of weighted aggregated sum product assessment. *Elektronika Ir Elektrotechnika*, *122*(6), 3–6. https://doi.org/10.5755/j01.eee.122.6.1810

Zhang, E. (2017). *Security and Analytics Experts Share the Most Important Cybersecurity Metrics and KPIs*. https://digitalguardian.com/blog/what-are-the-most-important-cybersecurity-metrics-kpis

Priedai

Priedas Nr. 1

Ekspertų apklausos anketa skirta klasikinių metrikų atrinkimui, kurios bus naudojamos agreguotoje metrikoje: *Užduotis: Toliau bus pateikiama 12 klausimų, kuriuose reikės išrinkti geriausias klasikines informacijos saugos metrikas. Atrinktos metrikos, vėliau bus naudojamos sudarant agreguotas informacijos saugos metrikas.*

Operacijų saugos metrikos:

1. Pasirinkite dvi svarbiausias metrikas:
   a) *Incidentai susiję su KPK (vnt.)*
   b) *KPK aptiktas el. laiškų sistemoje (vnt.)*
   c) *KPK aptiktas vartotojų lankomuose internetiniuose puslapiuose (vnt.)*
   d) *KPK platinančiuose internetiniuose puslapiuose*
   e) *KPK failai aptikti organizacijos įrenginiuose (įeina visi organizacijos įrenginiai) (vnt*
   f) *KPK failai aptikti organizacijos serveriuose (vnt.)*
   g) *KPK failai aptikti organizacijos darbuotojų kompiuteriuose (vnt.)*
   h) *KPK incidentai, reikalaujantys mechaniškai išvalyti sistemą (vnt.)*
2. Pasirinkite vieną svarbiausią metriką:
   a) *Pažeidžiamumus skenuojančia programine įranga nepadengiamos sistemos (vnt.)*
   b) *Žinomų pažeidžiamumų skaičius (vnt.)*
   c) *Laikas skiriamas pažeidžiamumo sutvarkymui (laikas)*
   d) *Randamų pažeidžiamumų skaičius per fiksuotą laiko vienetą (vnt.)*
3. Pasirinkite vieną svarbiausią metriką:
   a) *Rezervinio kopijavimo sistemos sutrikimų skaičius, įtraukiant duomenų kopijavimą ir atstatymą (vnt.)*
   b) *Rezervinio kopijavimo sistemos atsilikimas nuo nuostatos verčių, įtraukiant duomenų kopijavimą ir atstatymą (laikas)*
4. Pasirinkite vieną svarbiausią metriką:
   a) *Aktyviai nestebimos (monitoringas) ar nežurnalizuojamos kritinės organizacijos sistemos (vnt.)*
   b) *Reagavimo į žurnalinių įrašų ir monitoringo sistemų kritinius pranešimus laikas (laikas)*

Komunikacijų saugos metrikos:

5. Pasirinkite vieną svarbiausią metriką:
   a) *Ateinančių el. laiškų skaičius (vnt.)*
   b) *Aptikto šlamšto (angl. spam) kiekis (vnt.)*
   c) *Neaptikto šlamšto (angl. spam) kiekis (vnt.)*
6. Pasirinkite vieną svarbiausią metriką:
   a) *Ugniasienės taisyklių pakeitimai (vnt.)*
   b) *Ugniasienės eksploatavimui reikalingi darbo ištekliai (praleistas laikas val.)*
7. Pasirinkite vieną svarbiausią metriką:
   a) *Prisijungimai (sesijos) prie organizacijos internetu pasiekiamų serverių ir paslaugų (vnt.)*
   b) *Organizacijos tinklo srautas (B)*
   c) *Įrenginių esančių įmonės vidiniame tinkle skaičius (vnt.)*
8. Pasirinkite dvi svarbiausias metrikas:
   a) *Tinklo atakų skaičius (įtraukiamos sėkmingos ir nesėkmingos) (vnt.)*
   b) *Sėkmingų tinklo atakų skaičius (vnt.)*
   c) *Tinklo atakos MTTD (angl. mean time to detect) (laikas)*
   d) *Tinklo atakos MTTR (angl. mean time to repair) (laikas)*
   e) *Organizacijos tinklo įrenginių skenavimo iš išorės incidentų skaičius (vnt.)*

Sistemų įsigijimo, tobulinimo ir priežiūros metrikos:

9. Pasirinkite vieną svarbiausią metriką:
   a) *Sistemų neatitinkančių apibrėžtos konfigūracijos skaičius (vnt.)*
   b) *Sistemų konfigūracijos pakeitimų skaičius (vnt.)*
   c) *Sistemoms nepritaikytų konfigūracijos saugos griežtinimo (angl. security hardening) nustatymų skaičius (vnt.)*
10. Pasirinkite vieną svarbiausią metriką:
   a) *Sistemų neveikimo laikas, į kurį įeina planuotas ir neplanuotas sistemų neveikimas (laikas)*
   b) *Neplanuotas sistemų veiklos sutrikimas, dėl gedimų bei veiklos sutrikimų (laikas)*
   c) *Sistemų MTBF (angl. mean time between failures) (Atskleidžia sistemų patikimumą) (laikas)*
   d) *Sistemų MTTR (angl. mean time to repair) (laikas)*
11. Pasirinkite vieną svarbiausią metriką:
   a) *Kompiuterinės darbo vietos ir serveriai neturintys veikiančios antivirusinės programinės įrangos (vnt.)*
   b) *Kompiuterinės darbo vietos ir serveriai neturintys naujausių antivirusinės programinės įrangos KPK duomenų bazės sąrašų (vnt.)*
12. Pasirinkite vieną svarbiausią metriką:
   a) *Sistemos negavusios kritinių programinės įrangos atnaujinimų (vnt.)*
   b) *Laikas reikalingas kritiniams atnaujinimams įdiegti (laikas)*
   c) *Vėlavimas atlikti kritinį saugumo atnaujinimą (laikas)*
   d) *Kritiniams atnaujinimams ištestuoti skiriamas laikas (laikas)*

Priedas Nr. 2

Ekspertų apklausos anketa skirta kriterijų reikšmingumų nustatymui:

Užduotis: Žemiau pateiktose lentelėse pateikiami trys metriką apibūdinantys kokybės kriterijai: korektiškumas (angl. correctness), galimybė išmatuoti (angl. measurability) ir reikšmingumas (angl. meaningfulness). Įvertinkite kriterijus pagal pateiktas vertinimo skales.

Kriterijų reikšmių paaiškinimas:

Korektiškumas *(angl. correctness)* reiškia, kad metrika yra korektiškai taikoma ir nesuteikia jokios klaidingos informacijos, metrika yra gaunama be klaidų.

Galimybė išmatuoti *(angl. measurability)* reiškia, kad metrika turi galimų reikšmių sritį, aiškų skaitiniais vienetais apibrėžtą dydį.

Reikšmingumas *(angl. meaningfulness)* reiškia, kad metrika pateisina jai keliamus reikalavimus ir poreikius.

Kriterijų vertinimas metodu *AHP*

1 lentelė. Kriterijų porinio palyginimo matrica

Kriterijus A	Kriterijus B	Svarbesnis (A ar B)	Skalė (1-9)
Korektiškumas	Galimybė išmatuoti		
Korektiškumas	Reikšmingumas		
Galimybė išmatuoti	Reikšmingumas		

2 lentelė. Kokybinių kriterijų vertinimo skalė

Vertinimas (reitingas)	Vertinimo (reitingavimo) apibrėžimas	Vertinimo (reitingavimo) paaiškinimas
1	Alternatyvų svarba lygi	Abi alternatyvos kriterijaus atžvilgiu yra vienodos
3	Silpnai pranašesnė viena už kitą	Eksperto nuomone, alternatyva yra silpnai pranašesnė už kitą
5	Svarbus pranašumas	Eksperto nuomone, alternatyva yra svarbiai pranašesnė už kitą
7	Labai svarbus pranašumas	Eksperto nuomone, alternatyva yra labai svarbiai pranašesnė už kitą
9	Absoliučiai svarbus pranašumas	Eksperto nuomone, alternatyva yra neginčijamai pranašesnė už kitą
2, 4, 6, 8	Tarpinės reikšmės	Kai reikalingas kompromisas

Kriterijų vertinimas metodu *fuzzy TOPSIS*

3 lentelė. Kriterijų vertinimo lentelė

Kriterijus	Svarba
Korektiškumas	
Galimybė išmatuoti	
Reikšmingumas	
Galimi pasirinkimai: Labai žemas (LŽ), Žemas (Ž), Vidutiniškas žemas (VŽ), Vidutiniškas (V), Vidutiniškas aukštas (VA), Aukštas (A), Labai aukštas (LA)	

Priedas Nr. 3

Ekspertų apklausos anketa skirta metrikų reitingavimui atlikti:

Užduotis: Žemiau pateikiamos trys lentelės, kuriose pagal tris metriką apibūdinančius kokybės kriterijus korektiškumas (angl. correctness), galimybė išmatuoti (angl. measurability) ir reikšmingumas (angl. meaningfulness) reikia įvertinti informacijos saugos metrikas priskiriant joms lingvistines vertes, pagal pateiktą vertinimo lentelę.

1 lentelė. Lingvistiniai alternatyvų vertinimo terminai

Lingvistinis terminas
Labai žemas (LŽ)
Žemas (Ž)
Vidutiniškas žemas (VŽ)
Vidutiniškas (V)
Vidutiniškas aukštas (VA)
Aukštas (A)
Labai aukštas (LA)

2 lentelė. Operacijų saugos klasikinių informacijos saugos metrikų reitingavimo lentelė

Metrika	**Kriterijus**	**Svarba**
1. Incidentai susiję su KPK (vnt.)	Korektiškumas	
2. KPK failai aptikti organizacijos darbuotojų kompiuteriuose (vnt.)	Korektiškumas	
3. Laikas skiriamas pažeidžiamumo sutvarkymui (laikas)	Korektiškumas	
4. Rezervinio kopijavimo sistemos sutrikimų skaičius, įtraukiant duomenų kopijavimą ir atstatymą (vnt.)	Korektiškumas	
5. Reagavimo į žurnalinių įrašų ir monitoringo sistemų kritinius pranešimus laikas (laikas)	Korektiškumas	
1. Incidentai susiję su KPK (vnt.)	Galimybė išmatuoti	
2. KPK failai aptikti organizacijos darbuotojų kompiuteriuose (vnt.)	Galimybė išmatuoti	
3. Laikas skiriamas pažeidžiamumo sutvarkymui (laikas)	Galimybė išmatuoti	
4. Rezervinio kopijavimo sistemos sutrikimų skaičius, įtraukiant duomenų kopijavimą ir atstatymą (vnt.)	Galimybė išmatuoti	
5. Reagavimo į žurnalinių įrašų ir monitoringo sistemų kritinius pranešimus laikas (laikas)	Galimybė išmatuoti	
1. Incidentai susiję su KPK (vnt.)	Reikšmingumas	
2. KPK failai aptikti organizacijos darbuotojų kompiuteriuose (vnt.)	Reikšmingumas	
3. Laikas skiriamas pažeidžiamumo sutvarkymui (laikas)	Reikšmingumas	
4. Rezervinio kopijavimo sistemos sutrikimų skaičius, įtraukiant duomenų kopijavimą ir atstatymą (vnt.)	Reikšmingumas	
5. Reagavimo į žurnalinių įrašų ir monitoringo sistemų kritinius pranešimus laikas (laikas)	Reikšmingumas	

3 lentelė. Komunikacijų saugos klasikinių informacijos saugos metrikų reitingavimo lentelė

Metrika	Kriterijus	Svarba
1. Neaptikto šlamšto (angl. spam) kiekis (vnt.)	Korektiškumas	
2. Ugniasienės taisyklių pakeitimai (vnt.)	Korektiškumas	
3. Prisijungimai (sesijos) prie organizacijos internetu pasiekiamų serverių ir paslaugų (vnt.)	Korektiškumas	
4. Tinklo atakų skaičius (įtraukiamos sėkmingos ir nesėkmingos) (vnt.)	Korektiškumas	
5. Atakos MTTR (*mean time to repair*) (laikas)	Korektiškumas	
1. Neaptikto šlamšto (angl. spam) kiekis (vnt.)	Galimybė išmatuoti	
2. Ugniasienės taisyklių pakeitimai (vnt.)	Galimybė išmatuoti	
3. Prisijungimai (sesijos) prie organizacijos internetu pasiekiamų serverių ir paslaugų (vnt.)	Galimybė išmatuoti	
4. Tinklo atakų skaičius (įtraukiamos sėkmingos ir nesėkmingos) (vnt.)	Galimybė išmatuoti	
5. Atakos MTTR (*mean time to repair*) (laikas)	Galimybė išmatuoti	
1. Neaptikto šlamšto (angl. spam) kiekis (vnt.)	Reikšmingumas	
2. Ugniasienės taisyklių pakeitimai (vnt.)	Reikšmingumas	
3. Prisijungimai (sesijos) prie organizacijos internetu pasiekiamų serverių ir paslaugų (vnt.)	Reikšmingumas	
4. Tinklo atakų skaičius (įtraukiamos sėkmingos ir nesėkmingos) (vnt.)	Reikšmingumas	
5. Atakos MTTR (*mean time to repair*) (laikas)	Reikšmingumas	

4 lentelė. Informacinių sistemų įsigijimo, tobulinimo ir priežiūros srities klasikinių informacijos saugos metrikų reitingavimo lentelė

Metrika	Kriterijus	Svarba
1. Sistemoms nepritaikytų konfigūracijos saugos griežtinimo (angl. *security hardening*) nustatymų skaičius (vnt.)	Korektiškumas	
2. Sistemų MTTR (*mean time to repair*) (laikas)	Korektiškumas	
3. Kompiuterinės darbo vietos ir serveriai neturintys veikiančios antivirusinės programinės įrangos (vnt.)	Korektiškumas	
4. Sistemos negavusios kritinių programinės įrangos atnaujinimų (vnt.).	Korektiškumas	
1. Sistemoms nepritaikytų konfigūracijos saugos griežtinimo (angl. *security hardening*) nustatymų skaičius (vnt.)	Galimybė išmatuoti	
2. Sistemų MTTR (*mean time to repair*) (laikas)	Galimybė išmatuoti	
3. Kompiuterinės darbo vietos ir serveriai neturintys veikiančios antivirusinės programinės įrangos (vnt.)	Galimybė išmatuoti	
4. Sistemos negavusios kritinių programinės įrangos atnaujinimų (vnt.).	Galimybė išmatuoti	
1. Sistemoms nepritaikytų konfigūracijos saugos griežtinimo (angl. *security hardening*) nustatymų skaičius (vnt.)	Reikšmingumas	
2. Sistemų MTTR (*mean time to repair*) (laikas)	Reikšmingumas	
3. Kompiuterinės darbo vietos ir serveriai neturintys veikiančios antivirusinės programinės įrangos (vnt.)	Reikšmingumas	
4. Sistemos negavusios kritinių programinės įrangos atnaujinimų (vnt.).	Reikšmingumas	

Priedas Nr. 4

Alternatyvų ekspertinio vertinimo įverčiai:

1 lentelė. Operacijų saugos srities metrikų įverčiai (K – korektiškumas, GI – galimybė išmatuoti, R - reikšmingumas)

Metrika	**Krit.**	**E1**	**E2**	**E3**	**E4**	**E5**	**E6**	**E7**	**E8**	**E9**	**E10**
1. Incidentai susiję su KPK (vnt.)	**K**	V	VA	A	V	VŽ	VA	LA	VA	LA	VA
2. KPK failai aptikti organizacijos darbuotojų kompiuteriuose (vnt.)	**K**	LA	VA	LŽ	VA	V	A	LA	A	LA	V
3. Laikas skiriamas pažeidžiamumo sutvarkymui (laikas)	**K**	VA	VA	LA	V	A	VA	A	A	LA	VŽ
4. Rezervinio kopijavimo sistemos sutrikimų skaičius, įtraukiant duomenų kopijavimą ir atstatymą (vnt.)	**K**	Ž	V	VŽ	LA	A	A	LA	VA	LA	VŽ
5. Reagavimo į žurnalinių įrašų ir monitoringo sistemų kritinius pranešimus laikas (laikas)	**K**	A	VA	LA	LA	V	A	A	VA	LA	VŽ
1. Incidentai susiję su KPK (vnt.)	**GI**	VA	A	VŽ	A	VŽ	A	LA	A	LA	A
2. KPK failai aptikti organizacijos darbuotojų kompiuteriuose (vnt.)	**GI**	LA	A	V	LA	VA	A	LA	VŽ	LA	A
3. Laikas skiriamas pažeidžiamumo sutvarkymui (laikas)	**GI**	LA	A	LŽ	V	LA	VA	A	LA	V	Ž
4. Rezervinio kopijavimo sistemos sutrikimų skaičius, įtraukiant duomenų kopijavimą ir atstatymą (vnt.)	**GI**	Ž	Ž	LŽ	A	V	VA	A	LA	LA	VŽ
5. Reagavimo į žurnalinių įrašų ir monitoringo sistemų kritinius pranešimus laikas (laikas)	**GI**	A	A	LA	V	LA	VA	LA	LA	LA	VŽ
1. Incidentai susiję su KPK (vnt.)	**R**	VŽ	A	V	LA	VŽ	VA	LA	V	V	A
2. KPK failai aptikti organizacijos darbuotojų kompiuteriuose (vnt.)	**R**	LA	A	LŽ	LA	VA	V	LA	VA	VA	VA
3. Laikas skiriamas pažeidžiamumo sutvarkymui (laikas)	**R**	V	VA	VA	V	V	VA	LA	VA	VA	VA
4. Rezervinio kopijavimo sistemos sutrikimų skaičius, įtraukiant duomenų kopijavimą ir atstatymą (vnt.)	**R**	VŽ	VŽ	VŽ	A	V	A	LA	A	A	V
5. Reagavimo į žurnalinių įrašų ir monitoringo sistemų kritinius pranešimus laikas (laikas)	**R**	A	VA	LA	VA	VA	A	LA	LA	VA	A

2 lentelė. Komunikacijų saugos srities metrikų įverčiai (K – korektiškumas, GI – galimybė išmatuoti, R - reikšmingumas)

Metrika	**Krit.**	**E1**	**E2**	**E3**	**E4**	**E5**	**E6**	**E7**	**E8**	**E9**	**E10**
1. Neaptikto šlamšto (angl. spam) kiekis (vnt.)	**K**	VŽ	A	VŽ	VŽ	VŽ	VA	VA	V	LA	Ž
2. Ugniasienės taisyklių pakeitimai (vnt.)	**K**	Ž	A	VŽ	VA	LŽ	LA	A	LA	LA	V
3. Prisijungimai (sesijos) prie organizacijos internetu pasiekiamų serverių ir paslaugų (vnt.)	**K**	V	A	VŽ	LA	LA	A	A	A	VA	VŽ
4. Tinklo atakų skaičius (įtraukiamos sėkmingos ir nesėkmingos) (vnt.)	**K**	VŽ	VA	LA	VA	VA	VA	LA	V	LA	V
5. Atakos MTTR (*mean time to repair*) (laikas)	**K**	LA	A	V	V	VA	VA	LA	VŽ	LA	V
1. Neaptikto šlamšto (angl. spam) kiekis (vnt.)	**GI**	VA	VA	LŽ	V	Ž	A	VA	A	Ž	V
2. Ugniasienės taisyklių pakeitimai (vnt.)	**GI**	A	A	VA	VA	LA	LA	A	VŽ	LA	VA
3. Prisijungimai (sesijos) prie organizacijos internetu pasiekiamų serverių ir paslaugų (vnt.)	**GI**	VA	VA	VŽ	LA	LA	A	A	VA	LA	VŽ
4. Tinklo atakų skaičius (įtraukiamos sėkmingos ir nesėkmingos) (vnt.)	**GI**	VA	V	LA	A	V	A	LA	LA	A	V
5. Atakos MTTR (*mean time to repair*) (laikas)	**GI**	LA	VA	V	V	A	LA	LA	LA	A	Ž
1. Neaptikto šlamšto (angl. spam) kiekis (vnt.)	**R**	Ž	VA	V	V	Ž	A	VA	VA	A	VŽ
2. Ugniasienės taisyklių pakeitimai (vnt.)	**R**	Ž	VA	Ž	V	LŽ	LA	LA	LA	A	VA
3. Prisijungimai (sesijos) prie organizacijos internetu pasiekiamų serverių ir paslaugų (vnt.)	**R**	Ž	VA	VŽ	LA	Ž	A	A	LA	VA	V
4. Tinklo atakų skaičius (įtraukiamos sėkmingos ir nesėkmingos) (vnt.)	**R**	Ž	VA	LA	LA	V	LA	LA	A	LA	LA
5. Atakos MTTR (*mean time to repair*) (laikas)	**R**	LA	VA	V	V	VA	LA	A	LA	LA	A

3 lentelė. Sistemų įsigijimo, tobulinimo ir priežiūros saugos srities metrikų įverčiai

Metrika	**Krit.**	**E1**	**E2**	**E3**	**E4**	**E5**	**E6**	**E7**	**E8**	**E9**	**E10**
1. Sistemoms nepritaikytų konfigūracijos saugos griežtinimo (angl. *security hardening*) nustatymų skaičius (vnt.)	**K**	LA	VA	LA	V	Ž	A	A	VA	LA	Ž
2. Sistemų MTTR (*mean time to repair*) (laikas)	**K**	LA	A	V	VA	LA	VA	LA	A	A	VŽ
3. Kompiuterinės darbo vietos ir serveriai neturintys veikiančios antivirusinės programinės įrangos (vnt.)	**K**	V	V	LA	LA	LA	LA	A	V	LA	A
4. Sistemos negavusios kritinių programinės įrangos atnaujinimų (vnt.).	**K**	A	V	A	VA	A	A	LA	LA	LA	V
1. Sistemoms nepritaikytų konfigūracijos saugos griežtinimo (angl. *security hardening*) nustatymų skaičius (vnt.)	**GI**	LA	VA	LA	A	VŽ	VA	A	LA	A	Ž
2. Sistemų MTTR (*mean time to repair*) (laikas)	**GI**	LA	VA	VŽ	A	A	A	A	A	A	VŽ
3. Kompiuterinės darbo vietos ir serveriai neturintys veikiančios antivirusinės programinės įrangos (vnt.)	**GI**	LA	VA	LA	LA	LA	A	LA	LA	A	A
4. Sistemos negavusios kritinių programinės įrangos atnaujinimų (vnt.).	**GI**	LA	V	LA	A	A	A	A	LA	LA	V
1. Sistemoms nepritaikytų konfigūracijos saugos griežtinimo (angl. *security hardening*) nustatymų skaičius (vnt.)	**R**	LA	V	LA	A	VA	A	A	A	LA	VA
2. Sistemų MTTR (*mean time to repair*) (laikas)	**R**	LA	VA	LA	LA	A	LA	LA	VA	A	A
3. Kompiuterinės darbo vietos ir serveriai neturintys veikiančios antivirusinės programinės įrangos (vnt.)	**R**	VŽ	V	LA	LA	LA	LA	A	VŽ	LA	A
4. Sistemos negavusios kritinių programinės įrangos atnaujinimų (vnt.).	**R**	A	VA	A	A	V	LA	A	LA	LA	A

Priedas Nr. 5

Verifikavimo eksperimento anketa:

Užduotis: Žemiau pateikiamos dvi lentelės, kurias sudaro duomenys skirti organizacijos mėnesinėms informacijos saugos ataskaitoms ruošti. Pirmoji lentelė susideda iš duomenų, pateikiamų klasikinių informacijos saugos metrikų pavidalu. Antrojoje lentelėje pateikiami agreguotų informacijos saugos metrikų duomenys, apskaičiuoti iš pirmosios lentelės duomenų. Turint šiuos duomenis reikia paruošti dvi mėnesines organizacijos informacijos saugos ataskaitas. Pirmoji ataskaita turi būti sudaryta tik iš klasikinių informacijos saugos metrikų duomenų (naudojantis tik pirmąja lentele). Antroji tik iš agreguotų (naudojantis tik antrąja lentele). Atlikus ataskaitų ruošimą reikia atsakyti į žemiau pateikiamus 5 klausimus.

Pradiniai duomenys

		Mėnesio diena																															
Sritis	**Klasikinė metrika**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**Vidurkis**
Operacijų sauga	Incidentai susiję su KPK (vnt.)	6	4	4	6	3	5	7	1	8	5	1	8	10	6	10	4	4	2	0	9	6	4	0	1	10	2	2	1	4	7	10	4.83871
	KPK failai aptikti organizacijos darbuotojų kompiuteriuose (vnt.)	7	1	1	8	0	4	3	5	7	3	5	7	3	8	6	7	7	1	6	8	7	4	4	8	5	5	7	1	6	7	6	5.064516
	Laikas skiriamas pažeidžiamumo sutvarkymui (min)	95	18	51	31	25	220	68	157	18	131	233	199	206	21	129	266	5	231	50	120	226	199	48	298	272	289	173	49	152	217	298	145
	Rezervinio kopijavimo sistemos sutrikimų skaičius, įtraukiant duomenų kopijavimą ir atstatymą (vnt.)	8	8	1	7	10	4	10	8	10	2	5	2	7	8	10	7	0	3	5	9	2	2	1	7	0	6	2	7	4	10	5	5.483871
	Reagavimo į žurnalinių įrašų ir monitoringo sistemų kritinius pranešimus laikas (min)	22	89	43	77	19	46	41	27	12	2	23	79	9	85	28	84	6	28	98	21	66	81	32	91	48	7	43	44	38	83	40	45.54839
Komunikacijų sauga	Neaptikto šlamšto (angl. spam) kiekis (vnt.)	16	7	12	24	8	5	19	12	25	7	1	30	5	27	23	4	5	4	22	16	9	26	20	6	14	8	18	5	11	29	19	14.09677
	Ugniasienės taisyklių pakeitimai (vnt.)	9	0	5	0	5	0	1	9	7	3	1	3	0	3	1	5	4	9	2	2	0	5	7	9	2	8	1	0	10	1	6	3.806452
	Prisijungimai (sesijos) prie organizacijos internetu pasiekiamų serverių ir paslaugų (vnt.)	30527	87152	26548	47906	7729	87895	91555	57166	14372	52002	17818	49145	15081	73049	75929	60193	36241	89114	51982	11338	53523	30097	48105	47974	73406	38989	93159	94723	42865	33002	87848	52465.58
	Tinklo atakų skaičius (įtraukiamos sėkmingos ir nesėkmingos) (vnt.)	18	28	17	16	1	4	8	2	7	15	9	24	5	6	23	18	5	15	21	2	2	19	29	10	27	10	4	8	19	22	19	13.32258
	Atakos MTTR (Mean time to repair) (laikas)	13	36	170	118	35	32	48	10	27	90	65	120	99	20	184	68	198	5	76	100	49	136	146	168	139	48	5	6	21	64	1	74.09677
Sistemų sauga	Sistemoms nepritaikytų konfigūracijos saugos griežtinimo (angl. security hardening) nustatymų skaičius (vnt.)	4	10	4	2	7	5	5	10	8	0	3	8	7	9	5	1	3	1	6	6	8	2	4	10	1	5	4	6	3	3	10	5.16129
	Sistemų MTTR (Mean time to repair) (laikas)	5	0	4	8	1	6	7	7	8	5	7	6	8	7	4	0	6	6	3	6	0	3	5	3	7	8	5	4	4	1	8	4.903226
	Kompiuterinės darbo vietos ir serveriai neturintys veikiančios antivirusinės programinės įrangos (vnt.)	299	50	98	103	273	30	129	281	17	31	290	294	263	107	204	240	163	250	132	252	152	68	106	268	223	272	261	61	126	254	299	180.5161
	Sistemos negavusios kritinių programinės įrangos atnaujinimų (vnt.)	1	2	10	2	2	8	10	3	8	7	0	0	9	9	7	4	1	0	0	5	7	10	1	3	8	7	10	4	8	3	10	5.129032

1 pav. Pradiniai verifikavimo eksperimento duomenys skirti ataskaitos ruošimui (klasikinių metrikų duomenys)

	Mėnesio diena																															
Agreguota metrika	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**Vidurkis**
Operacijų saugos agreguota metrika	4.032	-10.4	-96.1	46.49	-84.5	2.87	5.121	-29.7	2.276	-87.6	-33.9	66.42	10.85	58.86	55.06	91.11	-104	-67.4	-2.57	47.43	44.38	13.07	-115	91.71	38.86	-21.8	-24.3	-79.2	-14.5	120.3	78.42	0.2
Komunikacijų saugos agreguota metrika	18.72	2.286	60.66	15.24	-102	-89.1	-23.5	-28	-25.8	-6.99	-102	88.4	-99.4	-25.5	110.2	10.35	18.24	23.03	26.25	-69.6	-104	78.05	141.4	78.87	86.44	-8.13	-65.1	-85.8	36.45	12.2	34.2	0.2
Sistemų saugos agreguota metrika	-74.3	-129	-57.8	-103	-87.3	-63	-9.02	14.09	-18.1	-127	-73.4	-37.7	45.72	12.66	-47.6	-143	-108	-113	-130	-22.6	-76.2	-94.3	-125	-31.5	-38.4	12.3	-4.82	-102	-77.2	-120	91.08	-59.25

2 pav. Pradiniai verifikavimo eksperimento duomenys skirti ataskaitos ruošimui (agreguotų metrikų duomenys)

Klausimynas

Klausimynu bus siekiama palyginti kuris būdas ruošiant informacijos saugos ataskaitą yra pranašesnis: remiantis klasikinėmis ar agreguotomis informacijos saugos metrikomis. Bus siekiama nustatyti 5 kriterijų reikšmingumus:

1) Ataskaitos ruošimo laiko – atskleidžia, kiek laiko užtrunka paruošti ataskaitą;

2) Ataskaitos ruošimo patogumo – atskleidžia ar patogus ataskaitos ruošimas;

3) Rezultatų suprantamumo – atskleidžia, kiek gauti rezultatai yra lengvai suprantami. Reikėtų atsižvelgti ir į tai, kad rezultatai galimai bus pristatinėjami organizacijos vadovybei, kuri gali neturėti gilių informacinių technologijų žinių;

4) Rezultatų reikšmingumas – atskleidžia, kiek gauti rezultatai yra reikšmingi ir leidžiantys pasiremti priimant organizacijos informacijos saugos sprendimus;

5) Ataskaitos kokybė – atskleidžia kaip gerai paruošta ataskaita apibūdins organizacijos saugumo padėtį.

Toliau pateikiami 5 klausimai:

Atsakymų skalė: [-5 – 5]
čia -5 reikštų taikant klasikines metrikas; 0 – vienoda reikšmė; 5 taikant agreguotas metrikas; -4,-3,-2,-1,1,2,3,4 – tarpinės reikšmės.

1) Kurios ataskaitos ruošimo laikas buvo trumpesnis?

2) Kurios ataskaitos ruošimas buvo patogesnis?

3) Kurios ataskaitos rezultatai lengviau suprantami?

4) Kurios ataskaitos rezultatai yra prasmingesni?

5) Kurios ataskaitos kokybė yra aukštesnė?