



VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

FUNDAMENTINIŲ MOKSLŲ FAKULTETAS

INFORMACINIŲ TECHNOLOGIJŲ KATEDRA

Roman Jevsejev

**IT RIZIKOS VALDYMO METODO PATOBULINIMAS TAIKANT
MATEMATINIO MODELIO ANALITINĮ METODĄ IR REZULTATŲ
SEGMENTAVIMO SPRENDIMUS**

**IMPROVEMENT OF IT RISK MANAGEMENT METHOD APPLYING THE
RESULTS SEGMENTATION SOLUTIONS AND ANALYTICAL MODEL OF
MATHEMATICAL METHOD**

Baigiamasis magistro darbas

ITVmit-17

studijų programa, valstybinis kodas

6211BX013

informatikos

studijų kryptis

Vilnius, 2019

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

FUNDAMENTINIŲ MOKSLŲ FAKULTETAS

INFORMACINIŲ TECHNOLOGIJŲ KATEDRA

TVIRTINU
Katedros vedėjas

(Parašas)

(Vardas, pavardė)

(Data)

Roman Jevsejev

**IT RIZIKOS VALDYMO METODO PATOBULINIMAS TAIKANT
MATEMATINIO MODELIO ANALITINĮ METODĄ IR REZULTATŲ
SEGMENTAVIMO SPRENDIMUS**

**IMPROVEMENT OF IT RISK MANAGEMENT METHOD APPLYING THE
RESULTS SEGMENTATION SOLUTIONS AND ANALYTICAL MODEL OF
MATHEMATICAL METHOD**

Baigiamasis magistro darbas

ITVmit-17

studijų programa, valstybinis kodas

6211BX013

informatikos

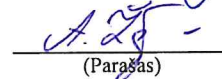
studijų kryptis

Vadovas prof. dr. Dalius Mažeika
(Pedag. vardas, vardas, pavardė)


(Parašas)

2019-05-21
(Data)

Konsultantas dr. Aušra Žemienė
(Pedag. vardas, vardas, pavardė)


(Parašas)

2019-05-21
(Data)

Vilnius, 2019

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
FUNDAMENTINIŲ MOKSLŲ FAKULTETAS
INFORMACINŲ SISTEMŲ KATEDRA

Informatikos inžinerijastudijų kryptis

Informacinių technologijųstudijų programa, valstybinis kodas
valdymas

.....specializacija

TVIRTINU
Katedros vedėjas

(Parašas)

(Vardas, pavardė)

(Data)

**BAIGIAMOJO MAGISTRO DARBO
UŽDUOTIS**

.....Nr.
Vilnius

Studentui (ei) Roman Jevsejev

(Vardas, pavardė)

Baigiamojo darbo tema:
IT rizikos valdymo metodo patobulinimas taikant matematinio modelio analitinį metodą
ir rezultatų segmentavimo sprendimus

patvirtinta 201...m. d. dekanų potvarkiu Nr.

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

BAIGIAMOJO DARBO UŽDUOTIS:

1. Įvertinti kibernetinės saugos situaciją ES ir Lietuvoje
2. Apžvelgti kibernetines grėsmes ir pažeidžiamumus
3. Apžvelgti ir palyginti esamas kibernetinių grėsmių rizikos vertinimo metodus
4. Sukurti ir pritaikyti IT rizikos valdymo metodą, atlikti organizacijos IT rizikos vertinimą ir remiantis gautais rezultatais, atlikti sukurto metodo analizę.

Baigiamojo darbo rengimo konsultantai:

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

Vadovas

.....
(Parašas)

Prof. dr. Dalius Mažeika

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

Užduotį gavau

.....
(Parašas)

.....
(Vardas, pavardė)

.....2017 10 15
(Data)

Vilniaus Gedimino technikos universitetas
Fundamentinių mokslų fakultetas
Informacinių technologijų katedra

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

Antrosios pakopos studijų **Informacinių technologijų valdymo** programos magistro baigiamasis darbas

Pavadinimas **IT rizikos valdymo metodo patobulinimas taikant matematinio modelio analitinį metodą ir rezultatų segmentavimo sprendimus**

Autorius **Roman Jevsejev**

Vadovas **Dalius Mažeika**

Kalba: lietuvių

Anotacija

Techninių rizikų vertinimui skiriama mažai dėmesio ir nėra objektyvių rizikos vertinimo aprašymų. Kadangi jos nereikalauja labai aukšto matematinio tikslumo, o svarbus yra rizikos egzistavimo faktas ir esamo fakto mastas, reikalingas analitinis metodas, kuris akivaizdžiai parodytų IT rizikos rezultatus.

Darbo tikslas – atlikti informacinių technologijų rizikos valdymo metodų analizę ir pasiūlyti metodo tobulinimo sprendimą, kuris leistu greitai ir tiksliai nustatyti IT rizikos reikšmę.

Darbo uždaviniai:

1. Nustatyti tinkamas kibernetinių grėsmių rizikos vertinimo metodikas, įvertinti kibernetinės saugos situaciją Europos Sąjungoje ir Lietuvoje.

2. Nustatyti kibernetinių grėsmių ir pažeidžiamumų kategorijas.

3. Apžvelgti ir palyginti esamas IT rizikos valdymo metodus, atliekant SSGG analizę.

4. Sukurti ir pritaikyti IT rizikos valdymo metodą, atlikti organizacijos IT rizikos vertinimą, remiantis gautais rezultatais atlikti sukurto metodo analizę, pateikti sistemų tobulinimo rekomendacijas bei išvadas.

Tyrimo objektas. IT rizikos valdymo metodai.

Tyrimo metodai. Tyrimą sudaro CRAM, OCTAVE, CORAS rizikų valdymo metodų stiprybių/silpnų, galimybių/grėsmių analizė, nustatomi metodų trūkumai. Parenkamas alternatyvus metodas, kuriam yra siūlomi patobulinimo sprendimai. Patobulintas metodas praktiškai pritaikomas organizacijoje. Atliekama gautų rezultatų analizė.

Darbo aktualumas. Darbo metu yra sukuriamas IT techninių rizikų valdymo metodas, kurio pagalba yra objektyviai nustatomos organizacijos rizikos, o rezultatai išreiškiami keturių segmentų skalėje (žemas, vidutinis, aukštas, labai aukštas rizikos lygis).

Darbo struktūra. Mokslinį darbą sudaro 4 dalys.

Darbo rezultatai. Patobulintas ir praktiškai pritaikytas matematinio modelio analitinis metodas. Nustatytos ir įvertintos organizacijos rizikos, atlikta rizikos jautrumo analizė. Išvardinti siūlomo metodo privalumai ir trūkumai, pateiktos rekomendacijos ir išvados.

Prasminiai žodžiai: IT rizikos; Metodas; Kibernetinis saugumas; Pažeidžiamumai; Grėsmės.

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

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

Master Degree Studies **Information Technology Management** study programme Master Graduation Thesis

Title **Improvement of IT Risk Management Method Applying the Results Segmentation Solutions and Analytical Model of Mathematical Method**

Author **Roman Jevsejev**

Academic supervisor **Dalius Mažeika**

Thesis language: Lithuanian

Annotation

Little attention is paid to technical risk assessment and there are no objective risk assessment descriptions. It doesn't require very high mathematical accuracy, but the importance of the existence of the risk and the extent of the existing fact are significant that is why an analytical method is needed to clearly demonstrate the results of IT risk.

Aim – Carry out an analysis of IT risk management methods and propose a method development solution that will allow quickly and accurately determine the significance of IT risk.

Tasks:

1. Evaluate the cyber security situation in the EU and LT and identify appropriate cyber threats risk assessment methods.
2. Distinguish categories of cyber threats and vulnerabilities.
3. Review and compare existing IT risk management methods performing SWOT analysis.
4. Develop and apply the IT risk management method; carry out the organization's IT risk assessment based on the results obtained. Thus, analyze the developed method and provide recommendations with necessary conclusions for system development.

Objects. IT risk management methods.

Research methods. The SWOT analysis of the risk management methods of CRAM, OCTAVE, CORAS and the potential threats of these methods. An alternative method is chosen for which improvement solutions are proposed. The improved method is practically applicable in the organization. The results analysis is done.

Relevance. During the research the IT technical risk management method was created which is used to objectively determine the risks of an organization and the results are expressed on a four-segment scale (low, medium, high, very high risk level).

Structure. The master thesis consists of 4 parts.

Results. An improved and practically applied mathematical model analytical method has been developed. The risk of the organization has been identified and assessed, and risk sensitivity analysis has been performed. The advantages and disadvantages of the proposed method, recommendations and conclusions have been enumerated.

Keywords: IT risk; Method; Cybersecurity; Assets; Threats.

(Baigiamojo darbo sąžiningumo deklaracijos forma)

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Roman Jevsejev, 20172004

(Studento vardas ir pavardė, studento pažymėjimo Nr.)

Fundamentinių mokslų fakultetas

(Fakultetas)

Informacinių technologijų valdymas, ITVmit-17

(Studijų programa, akademinė grupė)

BAIGIAMOJO DARBO (PROJEKTO)

SĄŽININGUMO DEKLARACIJA

2019 m. gegužės 17 d.

Patvirtinu, kad mano baigiamasis darbas tema „IT rizikos valdymo metodo patobulinimas taikant matematinio modelio analitinį metodą ir rezultatų segmentavimo sprendimus“ patvirtintas 2019 m. kovo 06 d. dekanų potvarkiu Nr. 147fm, yra savarankiškai parašytas. Šiame darbe pateikta medžiaga nėra plagijuota. Tiesiogiai ar netiesiogiai panaudotos kitų šaltinių citatos pažymėtos literatūros nuorodose.

Prenkant ir įvertinant medžiagą bei rengiant baigiamąjį darbą, mane konsultavo mokslininkai ir specialistai: profesorius daktaras Dalius Mažeika, Šarūnas Grigaliūnas, Tomas Zaleckas. Mano darbo vadovas profesorius daktaras Dalius Mažeika.

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


(Parašas)

Roman Jevsejev
(Vardas ir pavardė)

Turinys

Įvadas.....	10
1. Kibernetinės saugos apžvalga ir rizikos valdymo metodų analizė.....	12
1.1. Kibernetinės saugos apžvalga pasaulyje.....	12
1.2. Kibernetinės saugos apžvalga Europos Sąjungoje	13
1.3. Kibernetinės saugos apžvalga Lietuvos Respublikoje.....	14
1.4. Kibernetinės grėsmių ir pažeidžiamumų kategorijos	17
1.5. Matematinį rizikos vertinimo metodų analizė.....	19
1.6. IT rizikos samprata ir standartai	21
1.7. IT rizikos valdymo metodų apžvalga	23
1.7.1. CORAS metodas	23
1.7.2. OCTAVE metodas.....	25
1.7.3. CRAMM metodas	26
1.8. IT rizikos valdymo metodų SSGG analizė.....	28
2. IT rizikos valdymo metodo tobulinimo sprendimai	32
2.1. Siūlomo metodo tikslas ir reikalavimai	32
2.2. Siūlomo metodo sprendimai.....	33
3. Patobulinto IT rizikos valdymo metodo praktinis taikymas	39
3.1. IT rizikos apimtį nustatymas	39
3.1.1. IT infrastruktūros pagalba vykdomi šie įmonės procesai.....	40
3.2. Organizacijos techninės dokumentacijos analizė	41
3.2.1. Dokumentuose apibrėžti reikalavimai	42
3.3. Pažeidžiamumų ir grėsmių nustatymas	43
3.4. Personalo apklausa	44
3.5. Galimo žalos lygio, grėsmių realizavimo tikimybės ir rizikų įvertinimas	46
3.6. Rizikos rezultatų reitingavimas ir segmentavimas	48
3.7. Rizikos mažinimas.....	48
3.8. Rizikos jautrumo analizė	50
4. Metodo patobulinimo rezultatų analizė ir rekomendacijos	51
4.1. Patobulinto metodo privalumas.....	51
4.2. Patobulinto metodo trūkumai	52
4.3. Rekomendacijos	52
Išvados.....	53
Literatūros sąrašas	54
Priedai.....	58

Paveikslų sąrašas

1 pav. Nacionalinio kibernetinės saugos indekso rezultatai, 2019-02-19	16
2 pav. Nacionalinio kibernetinės saugos indekso sričių rezultatai, 2019-02-19	16
3 pav. Kiekybiniai rizikos valdymo metodai.....	19
4 pav. Rizikos vertinimo rodiklių sistema.....	21
5 pav. CORAS etapai	24
6 pav. Rizikos rezultatų reitingavimo skalė.....	37
7 pav. Atsakomųjų priemonių nustatymo forma (pavyzdys)	38
8 pav. Rizikų dinamikos grafikas (pavyzdys)	38
9 pav. Rizikos dinamika	50

Lentelių sąrašas

1 lentelė. Informacijos tinkamumo įvertinimas.....	18
2 lentelė. Rizikos valdymo metodikų SSGG charakteristikos.....	28
3 lentelė. CORAS metodikos SSGG	29
4 lentelė. OCTAVE metodikos SSGG	29
5 lentelė. CRAMM metodikos SSGG	30
6 lentelė. Siūlomo rizikos valdymo metodo sprendimai	34
7 lentelė. Galimo nuostolių lygio kriterijai (pavyzdys).....	36
8 lentelė. Grėsmių realizavimo tikimybės kriterijai (pavyzdys).....	37
9 lentelė. Nustatytos rizikos, grėsmės ir pažeidžiamumai pagal ISO/IEC 27005	43
10 lentelė. Personalo apklausos rezultatai	45
11 lentelė. Personalo apklausos rezultatų perskaičiuoti rezultatai	46
12 lentelė. Grėsmės realizavimo tikimybės skaičiavimai.....	46
13 lentelė. Galimo žalos lygio skaičiavimai	47
14 lentelė. Rizikos vertinimo rezultatai.....	47
15 lentelė. Rizikų segmentavimas	48
16 lentelė. Atsakomųjų priemonių nustatymo forma	49

Santrumpų sąrašas

IT	Informacinės technologijos
IT rizika	Informacinių technologijų rizika
IS	Informacinės sistemos bazių valdymo sistema
KS	Kompiuterinės sistemos (asmeniniai kompiuteriai)
DB	Duomenų bazė
VII	Valstybės informaciniai ištekliai
YSII	Ypatingos svarbos informacinė infrastruktūra
KAM	Krašto apsaugos ministerija
NKSC	Nacionalinis kibernetinio saugumo centras
VRM	Vidaus reikalų ministerija
ES	Europos Sąjunga
SSGG	Stiprybės / silpnybės, galimybės / grėsmės
PĮ	Programinė įranga

Ivadas

Informacinių technologijų taikymas bendruomenės socialiniuose ir kultūriniuose procesuose suformavo duomenų apsaugos nuo nesankcionuotos prieigos ir praradimo aspektą. Kuo aukštesnis socialinių procesų informatizavimo lygis, tuo didesnė rizika ir platesnis kibernetinės saugos grėsmių spektras duomenų nutekėjimo atžvilgiu. Europos Sąjungoje galiojančioje Pagrindinių teisių chartijoje yra pripažinta, kad kiekvienas asmuo turi teisę į jo asmens duomenų apsaugą. Chartijoje rašoma: „Asmens duomenys turi būti tinkamai tvarkomi ir naudojami tik konkrečiais tikslais ir tik atitinkamam asmeniui sutikus ar kitais nustatytais teisėtais pagrindais“ [1]. Daugelį metų teisės įgyvendinimas buvo reguliuojamas pagal 1995 m. Įsigaliojusią Duomenų apsaugos direktyvą [2]. Leistinas asmens interesų apsaugos aktyvumo lygis kibernetinio saugumo srityje pastaruoju metu sukelia daug ginčų, mokslinių diskusijų, susijusių su duomenų apsaugos tema.

IT technologijų plėtros konteksto atžvilgiu taikomi teisiniai įrankiai nesugeba išspręsti problemų, su kuriomis tenka susidurti visuomenei, antra vertus, tam tikrais atvejais yra stabdoma inovacijų plėtra. Siekdama atsižvelgti į šią problemą, Europos komisija inicijavo duomenų apsaugos reformą, atnaujino Duomenų apsaugos direktyvą ir 2008 m. patvirtintas Pamatinio sprendimo dėl duomenų, tvarkomų vykdant teisminį bendradarbiavimą baudžiamosiose bylose ir policijos bendradarbiavimą, apsaugos taisykles [3], kurių pagrindu tapo Bendrasis duomenų apsaugos reglamentas [4, 5]. Deja, tradiciniai administraciniai algoritmai ir reglamentai, kurių tikslas – suteikti duomenų apsaugą, kibernetinėje erdvėje veikia nepakankamai efektyviai.

Darbo problema. Informacinių sistemų ir technologijų plėtros intensyvumas reikalauja labai lanksčių ir adaptyvių kibernetinės saugos užtikrinimo metodų taikymo būdų [6]. Vienas iš šių metodų yra IT rizikos vertinimas, pvz., ISO / IEC 27005, BS 7799-3, NIST SP 800-39 ir kt. Šiuo metu nėra vienos metodologijos, kuria remiantis būtų galima efektyviai vertinti kibernetinių grėsmių riziką.

R. M. Stulz'as knygoje „Rizikos valdymo klaidos“ [7] pabrėžia, kad rizikos valdytojai kartais daro klaidų vertindami nuostolių tikimybę ar dydį. Tai įvyksta dėl neteisingo rizikos veiksmų paskirstymo. Įstaigai, turinčiai daugybę rizikų, skirtingų pozicijų koreliacija gali būti neteisingai įvertinta. Žinomos rizikos matavimas yra dažna rizikos valdymo praktikos problema.

Pasak R. M. Stulz'o, labai sunku įvertinti visas rizikas. Niekas negali nuspėti būsimų įvykių.

Darbo tikslas – atlikti informacinių technologijų rizikos valdymo metodų analizę ir pasiūlyti metodo tobulinimo sprendimą, kuris leistų greitai ir tiksliai nustatyti IT rizikos reikšmę.

Darbo uždaviniai:

- Įvertinti kibernetinės saugos situaciją Europos Sąjungoje ir Lietuvoje, nustatyti tinkamus kibernetinių grėsmių rizikos vertinimo metodus.

- Nustatyti kibernetinių grėsmių ir pažeidžiamumų kategorijas.
- Apžvelgti ir palyginti esamus IT rizikos valdymo metodus, atliekant SSGG analizę.
- Sukurti ir pritaikyti IT rizikos vertinimo metodą, atlikti organizacijos IT rizikos vertinimą, remiantis gautais rezultatais, atlikti sukurto metodo analizę, pateikti sistemų tobulinimo rekomendacijas bei išvadas.

Tyrimo objektas. IT rizikos valdymo metodai.

Tyrimo metodai. Tyrimą sudaro CRAM, OCTAVE, CORAS rizikų valdymo metodų stiprybių/silpnybių, galimybių/grėsmių analizė, nustatomi metodų trūkumai. Parenkamas alternatyvus metodas, kuriam yra siūlomi patobulinimo sprendimai. Pakeistas metodas praktiškai pritaikomas organizacijoje. Atliekama gautų rezultatų analizė.

Darbo aktualumas. Darbo metu yra sukuriamas IT techninių rizikų valdymo metodas, kuris objektyviai nustato organizacijos rizikas, rezultatai pateikiami keturių lygių skalėje (žemas, vidutinis, aukštas, labai aukštas rizikos lygis).

Darbo struktūra. Mokslinį darbą sudaro 4 dalys. Pirmoje dalyje nagrinėjama kibernetinė sauga pasaulyje, Europos Sąjungoje ir Lietuvoje, šią sritį reglamentuojantys IT rizikos standartai, atliekama IT rizikos valdymo metodų SSGG analizė. Antroje dalyje aprašomi techninių IT rizikų valdymo metodo patobulinimo sprendimai, pateikiami rizikos vertinimo kūrimo procesai ir metodologija. Trečioje dalyje aprašoma, kaip patobulintas metodas pritaikomas praktikoje, pateikiama įmonės charakteristika, atliekama įmonės IT dokumentacijos analizė, nustatomos objektyvios su IT infrastruktūra susijusios rizikos, vykdoma IT specialistų apklausa, kurios metu nustatomos rizikos vertinimo kriterijų reikšmės. Atliekamas rizikos vertinimas, mažinimas ir dinamikos stebėjimas. Ketvirtoje dalyje analizuojami metodo rezultatai ir diskusija. Penkta dalis skirta darbo išvadoms ir rekomendacijoms apibendrinti. Prieduose pateikti IT rizikų valdymo metodų SSGG analizės rezultatai, ISO/IEC 27005 standarto „C“ ir „D“ priedas (lietuvių k.), apklausos anketos pavyzdys ir apklausos vertinimo metodika.

1. Kibernetinės saugos apžvalga ir rizikos valdymo metodų analizė

Kibernetinės saugos klausimas šiuolaikiniame pasaulyje yra itin svarbus. Šiam apibrėžimui atsiradus kilo poreikis atskirti kibernetinės saugos sąvoką nuo informacijos saugos. Melisa Stevens‘a 2016 m. straipsnyje „Ar yra skirtumas tarp informacinės ir kibernetinės saugos“ teigia, kad kibernetinė sauga yra informacijos saugos rūšis, kurios paskirtis yra saugoti duomenis elektronine forma ir nustatyti duomenų svarbą, nurodyti, kur jie yra saugomi ir kokias technologijas būtina taikyti juos apsaugant [8].

J. Gospodariko ir M. Paškovskajos 2016 m. knygoje „Tarptautinė saugos ekonomika“ rašoma: „Kibernetinė sauga yra kibernetinės erdvės apsaugos išteklių ir būdų visuma, kurią sudaro strategijos, saugos aprūpinimo principų, saugos garantijos, rizikos valdymo metodų, veiksmų ir patirties, draudimo ir technologijų, organizacijų resursų ir vartotojų priemonių rinkinys“ [8].

Kibernetinės saugos sričiai priskiriamos apsaugos priemonės ir veiksmai, kuriuos atlikus užtikrinama kibernetinės erdvės apsauga ekonominėje, civilinėje ir karinėje srityse.

1.1. Kibernetinės saugos apžvalga pasaulyje

Informacinių technologijų tinklas apima įvairias sritis, pvz., el. bankininkystę, valstybės infrastruktūras ir kt. Dėl šios priežasties atsirado didelis kibernetinės saugos poreikis. Dauguma įmonių saugo savo duomenis serveriuose, asmeniniuose ir nešiojamuose kompiuteriuose arba el. debesijos erdvėje. Kibernetinėje erdvėje aktyviai veikia įvairios kibernetinių nusikaltėlių (įsilaužėlių) grupės ir tarptautiniai teroristai. Šnipinėdami ekonominėje, civilinėje ir karinėje srityse, jie bando sutrikdyti įmonių, įstaigų, organizacijų ir kitų IT infrastruktūrą turinčių objektų veiklą [9]. 2019 metų sausio pradžioje yra užfiksuotos 47 kibernetinės atakos [10].

Pasekmė – kibernetinių užpuolimų žala gali viršyti ekonominių sankcijų ir karinių konfliktų nuostolius. Remiantis Interpolo duomenimis, 2012 m. Europos Sąjungoje žala dėl kibernetinių nusikaltimų sudarė daugiau nei 750 mlrd. EUR.

- 2016 m. tinklalapyje www.rheagroup.com pateikiami duomenys apie didžiausius 2016 metų kibernetinius nusikaltimus:
- 2016 m. vasario mėn. Bangladešo centrinio banko užpuolimas, kurio metu žala sudarė \$81 mln. ir buvo išvengta dar \$850 mln. vagystės;
- 2016 m. rugpjūčio mėn. interneto tinkluose buvo paskelbti 200 mln. „Yahoo“ vartotojų asmeniniai ir prisijungimo duomenys, tarp kurių buvo vardai, slaptažodžiai, gimimo datos. Duomenų kainą sudarė tik 3 BTC, tai yra \$1,860 [11].

Greta kibernetinių nusikaltėlių veiklos, labai aktuali yra asmens duomenų ir socialinių tinklų naudotojų apsauga nuo slapto informacijos rinkimo. Priklausomai nuo tinklo naudotojų individualių

pomėgių, polinkių, informacija gali būti plačiai naudojama platinant reklamą, interneto paslaugų pardavimo srityje ir politiniais tikslais. Kiekvienam žmogui yra svarbu suprasti tinkle ir laikmenose esančių asmens duomenų saugos svarbą, praradimo ir paviešinimo riziką. Dėl saugumo užtikrinimo problemų vyksta banko duomenų, asmeninės ir kitos informacijos vagystės.

Globalioje 2018 m. Ženevos kibernetinės saugos rodiklių ataskaitoje [12] skelbiama, kad nacionalinių ir Europos kibernetinės saugos strategijų santykio klausimas yra mokslinė teorinė ir praktinė problema, apibūdinama kaip didelis Europos Sąjungos šalių socialinės, ekonominės ir technologijų plėtros lygio skirtumas. Tokia padėtis lemia nepakankamai patikimą kibernetinės saugos strategiją daugelyje Europos Sąjungos šalių. Nepaisant Europos Komisijos reikalavimų kuo skubiau sukurti nacionalinę kibernetinės saugos aprūpinimo strategiją, dauguma šalių tai įvykdė formaliai, neįgyvendindamos realizavimo priemonių, nes šis procesas reikalauja didelių finansinių išteklių. Neturtingos Europos Sąjungos šalys, pvz., Bulgarija, Rumunija, Graikija, Portugalija, negali sau leisti įsigyti šių priemonių. Šios šalys išsiskiria žemu interneto naudojimo intensyvumu ir skaitmeninės ekonomikos lygiu.

Ataskaitoje šalys palyginamos pagal kibernetinio saugumo lygį, įvertinant šiuos šalies rodiklius:

- teisinis: juridinių asmenų ir institucijų, atsakingų už kibernetinį saugumą ir elektroninius nusikaltimus, įvertinimas;
- techninis: techninių institucijų ir struktūrų, dirbančių su kibernetine sauga, egzistavimo įvertinimas;
- organizacinis: kibernetinės saugos nacionalinio lygio plėtros strategijos įvertinimas;
- pajėgumų stiprinimas: mokslinių tyrimų ir plėtros, išsilavinimo ir mokymo programų, sertifikuotų specialistų agentūrų ir valstybės sektorių, skatinančių pajėgumų stiprinimą, įvertinimas;
- bendradarbiavimas: partnerystės, kooperatinės sistemos ir informacijos mainų tinklai.

1.2. Kibernetinės saugos apžvalga Europos Sąjungoje

Bandymai sukurti bendrą Europos Sąjungos kibernetinės saugos politiką vyksta du dešimtmečius. Siekiant valdyti globalų kompiuterinį tinklą ir kibernetinių nusikaltimų užkardymo procesus, 2001 m. Budapešte priimta Europos Tarybos kibernetinių nusikaltimų konvencija (toliau – Konvencija). 2003 m. priimtas Kibernetinių nusikaltimų konvencijos papildomas protokolai. Nors Konvencijoje tarptautiniu lygmeniu buvo skirta daug dėmesio šalių veiksams koordinuoti, dėl nesankcionuotų įsibrovimų į kompiuterines sistemas tai nebuvo efektyvus kibernetinės saugos

užtikrinimo įrankis Europos Sąjungoje. Konvencijoje nebuvo aprašyti konkretūs mechanizmai, įrankiai, teisinių aktų realizavimo ir valdymo būdai nacionaliniu lygmeniu.

Siekiant koordinuoti ir nukreipti šalių kibernetinio priešinimosi veiklą, 2004 m. buvo įsteigta Europos tinklo ir informacijos saugos agentūra (European Network and Information Security Agency, ENISA) [13].

2010 m. buvo organizuoti pirmi kibernetinės saugos mokymai, kuriuose dalyvavo 170 specialistų iš 22 šalių [14]. 2013 m. pradėjo veikti Europos kibernetinių nusikaltimų kovos centras (European Cybercrime Centre, ECC), kuris regioniniame ir tarptautiniame lygmenyje teikia informacinį, operatyvinį ir ekspertinį kibernetinių nusikaltimų tyrimų užtikrinimą. Centrai buvo išskirti kibernetinės saugos tendencijų nustatymo uždaviniai: prisidėti prie informacijos tarp ES šalių apsikeitimo, analizuoti nacionaliniu lygmeniu priimtas prevencines priemones ir veiksmus, ruošti kibernetinės srities policijos, teismų ir prokuratūros darbuotojus [15].

2013 metais pristatyta ES kibernetinė strategija „Atvira ir saugi kibernetinė erdvė“ [16]. ES kibernetinės strategijos tikslas – ES šalių kibernetinio saugumo potencialo ir patvarumo didinimas, efektyvios kibernetinės saugos aprūpinimo infrastruktūros formavimas, kibernetinės saugos tarptautinio koordinavimo principų kūrimas.

2016 m. rugpjūčio mėnesį buvo patvirtinta ir įsigaliojo ES kibernetinės saugos direktyva [17, 18]. Vadovaujantis šia direktyva, ES šalys kartu su ENISA sukūrė grupę, kurios funkcijos – duomenų siuntimas, keitimasis informacija, kibernetinės saugos grėsmių ir incidentų prevencija. 2016 metais kuriamas Bendrasis duomenų apsaugos reglamentas (General Data Protection Regulation, GDPR). 2017 metais yra įvedamas skaitmeninės produkcijos ir paslaugų sertifikavimas. 2018 metų gegužės 25 d. įsigaliojo Bendrasis duomenų apsaugos reglamentas [19]. Reglamento įgyvendinimas turėjo didelę įtaką užtikrinant Lietuvos kibernetinį saugumą.

1.3. Kibernetinės saugos apžvalga Lietuvos Respublikoje

Kibernetinės saugos užtikrinimas Lietuvoje yra viena iš Krašto apsaugos ministerijos (toliau – KAM) veiklų. Procesai ir IT saugumas valstybiniame sektoriuje tapo centralizuoti, kai Lietuvoje registrai ir kadastrai buvo pradėti valdyti informacinių sistemų, tačiau esami įstatymai reglamentavo informacinių sistemų tvarką fragmentiškai ir nepakankamai nuosekliai. Taip atsirado įstatymo, kuris sujungtų visas tvarkas į vieną, poreikis, taip pat reikėjo atsisakyti nereikalingų įstatymų. Tuomet 2011 m. gruodžio 15 d. buvo priimtas Valstybės informacinių išteklių (toliau – VII) ir ypatingos svarbos informacinės infrastruktūros (toliau – YSII) valdymo įstatymas [20, 21]. Tokių teisės normų poreikis tapo ne tik nacionalinio, bet ir tarptautinio lygmens, kadangi IT tobulėjo greičiau negu teisinė dalis ir teisinis reglamentavimas neatitiko pokyčių.

Europos mastu kibernetinės saugos užtikrinimas Lietuvoje yra Nuolatinio struktūrizuoto bendradarbiavimo (PESCO) iniciatyva [22]. Įsigaliojus Kibernetinio saugumo įstatymui (2014 m. gruodžio 11 d. Nr. XII-1428), 2015 m. sausio 1 d. kaip atskiras juridinis asmuo prie KAM pradėjo veikti Nacionalinis kibernetinio saugumo centras (toliau – NKSC), kuris:

- įgyvendina kibernetinės saugos politiką;
- valdo valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros kibernetinės saugos incidentus;
- rengia techninius ir organizacinius kibernetinės saugos reikalavimus;
- teikia pasiūlymus krašto apsaugos ministrui;
- atlieka VII ir YSII atitikties reikalavimams stebėseną;
- teikia konsultacijas ir rekomendacijas VII ir YSII valdytojams;
- analizuoja nacionalinę kibernetinės saugos situaciją ir teikia ataskaitas.

2017 m. Lietuvoje buvo atliktas kibernetinės saugos lygio vertinimas. Oksfordo universiteto Pasaulinis kibernetinio saugumo kompetencijos centras, remdamasis sukurtu kibernetinio brandumo modeliu (angl. Cybersecurity Maturity Model), ištyrė kiekvieną modelio sudedamąją dalį:

- kibernetinio saugumo strategiją, rengimo stadijas ir politikos, kultūros bei visuomenės teisinį reguliavimą;
- verslo modelį ir technologijų integralumą.

Bendra Lietuvos kibernetinės saugos branda buvo įvertinta „vidutiniškai“. 2018 m. sausio 1 d. įgyvendintas kibernetinio saugumo ir elektroninių ryšių tinklų saugos padalinių ir funkcijų konsolidavimas, sujungęs Informacinių technologijų tarnybą, Vyriausybinių ryšių centrą ir Ryšių reguliavimo tarnybos Saugumo incidentų tyrimų padalinį (CERT-LT) bei kibernetinio saugumo specialistus.

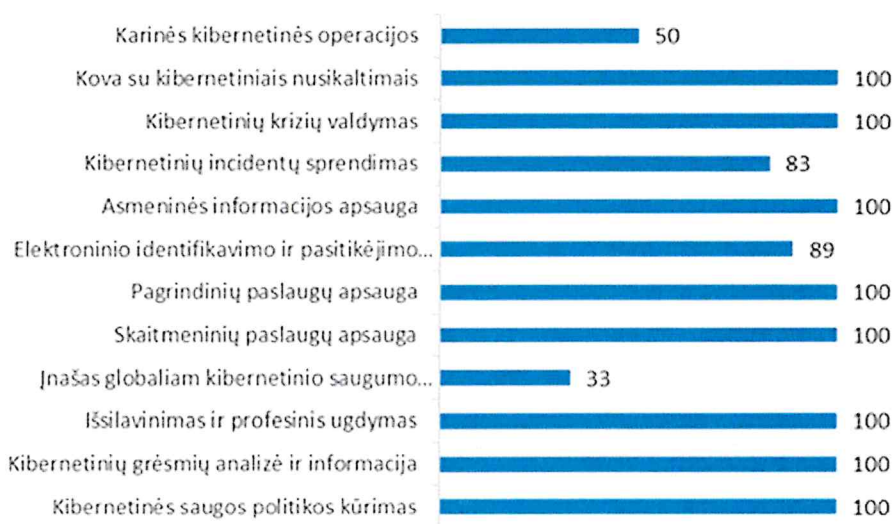
Nuo 2018 m. sausio 1 d. ypatingos svarbos informacinė infrastruktūra (YSII) Kibernetinio saugumo įstatyme apibrėžta kaip privataus ar viešojo administravimo subjekto valdoma informacinė infrastruktūra. Įvykus kibernetinės saugos incidentui, gali kilti didelė žala nacionaliniam saugumui, šalies ūkiui, valstybės ir visuomenės interesams. YSII ir VII valdytojų bei tvarkytojų valdomos infrastruktūros stebėseną davė akivaizdžių rezultatų – buvo rasta ir neutralizuota daugiau nei keturi šimtai standartinėmis saugumo užtikrinimo priemonėmis neaptinkamos žalingos programinės įrangos veikimo atvejų [23].

Pagal nacionalinio kibernetinės saugos indekso rezultatus (2019-02-19, 12:45) Lietuva yra tarp Čekijos, Ispanijos ir Estijos [24]. Indeksas yra lygus 88,31, o pirmos vietos indeksas yra 90,91. Rezultatai pateikti 1 paveiksle.



1 pav. Nacionalinio kibernetinės saugos indekso rezultatai, 2019-02-19

Aukštas nacionalinio kibernetinės saugos indekso rezultatas rodo Lietuvos pastangas užtikrinant kibernetinę saugą. Indeksas apima sritis, pavaizduotas 2 paveiksle.



2 pav. Nacionalinio kibernetinės saugos indekso sričių rezultatai, 2019-02-19

Pasak prof. Laimučio Telksnio, kibernetiniai nusikaltimai yra rengiami prieš valstybės institucijas (2016 metų mokslinis priedas „Kibernetinio saugumo apžvalga“ [25]). Kibernetinio saugumo procesai nuolat vertinami Valstybės kontrolės inspekcijos. Ypatingos svarbos valstybės informacinių išteklių valdymo ataskaitoje 2018 m. birželio 28 d. Nr. VA-2018-P-900-3-6 rašoma, kad „kibernetinės saugos sistema ir jos taikymas nepakankamai efektyvus, poreikiai ir rizikos yra vertinamos netinkamai“ [26].

2017 m. CERT-LT duomenimis, yra dvi didžiausios kibernetinės saugos problemos: kenkimo programinė įranga (kenkimo kodai) ir nesaugios informacinės sistemos, įskaitant interneto svetaines.

Pasak LITNET vadovo Šarūno Grigaliūnio, „šiandien esame visiškai priklausomi nuo duomenų srautų ir socialinės informacijos. Faktiškai turime dvi grėsmes – duomenų pasiekiamumo ir šaltinio patikimumo. Geltonoji žiniasklaida, propaganda ir duomenų nutekinimas yra pagrindinės prekės bei pagrindiniai taikiniai. Artimiausiu laiku į tinklą bus sujungta daugybė įrenginių, kurių informacijos koreliacijos išėiga taps kita didžiule problema“ [2019-01-18].

1.4. Kibernetinės grėsmių ir pažeidžiamumų kategorijos

Didžiausia organizacijų problema – kibernetinės grėsmės. IT saugos žodynelyje RFC 2828 [27] kibernetinė grėsmė yra apibūdinama kaip pavojus, pažeidžiantis IT saugą ir kenkiantis IT infrastruktūroms. Kibernetinė grėsmė skirstoma į dvi kategorijas:

- tyčinė (kai įvyksta asmens arba nusikalstamos organizacijos įsilaužimas),
- atsitiktinė (kai sutrinka pati kompiuterinių sistemų veikla arba jas paveikia gamtos reiškiniai).

Grėsmės įvairiuose literatūros šaltiniuose apibrėžiamos skirtingai. ISO 27005 standartuose grėsmė apibrėžiama kaip galima incidento priežastis, kuri gali pakenkti sistemoms ir organizacijoms [28]. Jungtinių Amerikos Valstijų NIST „Federalinių informacijos apdorojimo standartų (toliau – FIPS) 200, minimalių saugumo reikalavimų federalinėms ir informacinėms sistemoms“ aprašuose [29] grėsmė yra susieta su informacijos užtikrinimu bei apibrėžiama kaip „aplinkybės arba įvykiai, turintys potencialiai neigiamą poveikį organizacijos veiklai (įskaitant misiją, funkcijas, įvaizdį ar reputaciją), organizaciniam ar asmens turtui, naudojant neteisėtą prieigą prie informacinių sistemų, sunaikinant, atskleidžiant, pakeičiant informaciją arba paslaugą.“

Grėsmės šaltinis gali sėkmingai išnaudoti tam tikrą informacinės sistemos pažeidžiamumą. Pažeidžiamumas pats nekenkia, turi būti grėsmė, leidžianti išnaudoti šį pažeidžiamumą. Grėsmės nesukelia rizikos be pažeidžiamumo išnaudojimo, tačiau jas reikia rasti ir stebėti pokyčius. Grėsmė be pažeidžiamumo sukelia riziką. Pažeidžiamumai ir grėsmės nustatomi pagal ISO 27005 standarto priedą „C“ („Tipinių grėsmių pavyzdžiai“) ir priedą „D“ („Pažeidžiamumai ir jų vertinimo metodai“) [28]. Išvardinti standarto priedai išsamiai pateikti šio darbo 2 ir 3 priede bei 1–4 lentelėse.

2005 m. Vidaus reikalų ministerijos leidinyje „Rizikos vadovas“ [30] pateiktos kelios kibernetinių grėsmių kategorijos:

- duomenų klasifikacija (duomenų rinkimas arba koncentracija, dėl kurių galimas neteisingas interpretavimas, slapta manipuliavimas kanalais arba kenkėjiško kodo naudojimas);
- personalas (neteisėtas arba nevaldomas prisijungimas prie sistemų, kenkėjiški darbuotojų veiksmai arba informacijos klastojimas);
- programinė įranga (neefektyvi saugos programinė įranga, sukelianti procedūrines klaidas);

- kriminalas (fizinis įrangos sunaikinimas, informacijos vagystė, ginkluotas apiplėšimas arba fizinė žala personalui);
- aplinka (infrastruktūros gedimas, paslaugų tiekimo sutrikimai, stichinės nelaimės ir kt.);
- IT infrastruktūra (techninės įrangos gedimai, programinės įrangos veikimo sutrikimai, operacinės sistemos sutrikimai, ryšių sistemos gedimai);
- įsipareigojimų įgyvendinimo vėlavimas (produktyvumo sumažėjimas, lemiantis pajamų mažėjimą, išlaidų augimą arba delspinigius).
- Duomenų šaltiniai skaidomi į tris kategorijas pagal informacijos tinkamumo įvertinimą, kuris pateiktas 1 lentelėje.

1 lentelė. Informacijos tinkamumo įvertinimas

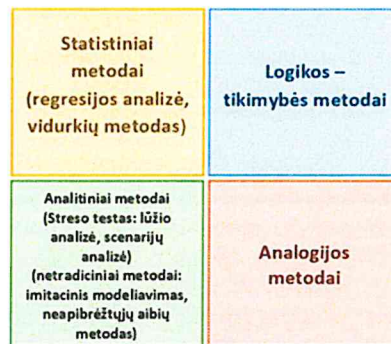
	Pirminiai	Antriniai	Tretiniai
Apibrėžimai	Šaltiniai, kuriuose yra neapdorota, originali, neinterpretuota ir neįvertinta informacija	Šaltiniai, kurie sumuoja, analizuoja, vertina ir interpretuoja informaciją, paimtą iš pirminių šaltinių. Paprastai jie būna aiškinamojo pobūdžio	Šaltiniai, kurie kompiliuoja, analizuoja ir sumuoja antrinius šaltinius. Paprastai jie faktiniai
Pavyzdžiai	Įvykių registras, operatoriaus prisijungimų registras ir pastabos, tinklo skanavimo duomenys, techninė dokumentacija, atvejai, korespondencija, interviu	Kritika ir interpretacija, istorija, vyriausybės politika, įstatymai, moraliniai ir etiniai aspektai, politiniai aspektai, politika ir vyriausybės sprendimai, psichologiniai aspektai, viešoji nuomonė, religija, religiniai aspektai, socialinė politika, studijos ir mokymai	Santraukos, bibliografija, chronologija, klasifikacija, žodynai, enciklopedijos, direktorijos, vadovėliai, instrukcijos, vadovai ir pan., identifikacijos indeksai, registrai, statistika, lentelės

Nacionalinio standartizacijos ir technologijų instituto (toliau – NIST) mokslininkai skaido grėsmių šaltinius į tris kategorijas pagal rizikos lygį:

- **aukštas (high)** – grėsmių šaltinis aktyvus, pažeidžiamumo išnaudojimo prevencija neefektyvi;
- **vidutinis (medium)** – grėsmių šaltinis aktyvus, pažeidžiamumo išnaudojimo prevencija efektyvi;
- **žemas (low)** – grėsmių šaltinis nėra motyvuotas ir nesukelia grėsmės, pažeidžiamumo išnaudojimo priemonės veikia efektyviai.

1.5. Matematinų rizikos vertinimo metodų analizė

Rizikos vertinimui naudojami kiekybiniai ir kokybiniai metodai. Matematinis modeliavimas priskirtas kiekybiniais metodams. Kokybiniai metodai kompleksiskai įvertina rizikos įgyvendinimo tikimybę ir jos realizavimo pasekmes. Tokie metodai reikalauja kompetentingų ekspertinių žinių ir tai yra pagrindinis trūkumas. Kiekybiniai metodai yra sudėtingi vertinimo procesų atžvilgiu, bet leidžia nustatyti kelias alternatyvas priimant sprendimus. Kiekybiniai metodai yra pateikti 3 paveiksle.



3 pav. Kiekybiniai rizikos valdymo metodai

Statistiniai metodai rizikos vertinimui naudojami dažniausiai (regresijos analizė, vidurkių metodas). Šie metodai paremti atsitiktinių įvykių įgyvendinimo skaičiavimais. Skaičiavimo paprastumas yra statistinių metodų privalumas. Šio metodo trūkumas – didelis retrospektyvinių duomenų kiekio poreikis.

Logikos–tikimybės metodai tapo naudojami neseniai. Ekonomikoje šie metodai taikomi bankininkystės srityje. Šie metodai yra sukurti kaip tikimybinių, loginių ir struktūrinių kreditinių rizikų modeliai, nes apskaičiuota kredito rizikos kaina ir rizikos lygis.

Analogijų metodai paremti rizikos vertinimo duomenų bazių analizės principu, kadangi yra palyginami objektai–analogai. Tiriamo objekto informacijos suderinamumas su analogišku objektu yra svarbiausia šio metodo taikymo sąlyga. Metodas taikomas dažnai vertinant besikartojančius įvykius arba objektų riziką.

Analitinių metodų grupė dažniausiai naudojama vertinant investicinių ir inovacinių projektų riziką ir yra skirstoma į du pogrupius:

- tikimybinių paskirstymo neįvertinantys metodai (streso testas, lūžio, ir scenarijų analizė);
- tikimybinių paskirstymą įvertinantys metodai (netradiciniai metodai).

Matematiniai modeliai ir metodai priklauso analitinių metodų grupei. Pagrindinis matematinio modeliavimo taikymo tikslas yra įvertinti bendrą riziką: $R = f(P, I)$, kur P – rizikos įvykio įgyvendinimo tikimybė, I – veiksmų įtakos potencialios pasekmės [31].

Matematiniai modeliai pagal užduotį ir turimą pradinę informaciją skaidomi į determinuotus, stochastinius, lingvistinius ir lošimo tipo modelius.

Lošimo (nestochastiniai) modeliai naudojami tik tuomet, kai trūksta pradinės informacijos taikant kitus modelius. Lošimo teorijos pagrindu formuojami keli galimi rizikos įvykio rezultatai. Statistiniai ir strateginiai lošimai nustato rizikos lygį ir įgyvendinimo tikimybę.

Lingvistinių modelių pagrindas – nelyginės logikos metodai. Neapibrėžtumas įvardijamas kaip priklausomybės funkcija, kuriai nebūtinai įvykių pasikartojimas. Numatoma, kad šių metodų taikymas reikalauja ekspertinio neapibrėžtumo lygio vertinimo.

Stochastiniai modeliai remiasi statistinių skaičiavimų taikymo ir pakankamos statistinės informacijos dėl tam tikro įvykio egzistavimo pagrindu. Stochastiniais modeliais nustatytose ribose yra vertinama rizikos įgyvendinimo tikimybė. Šie modeliai taikomi rizikos veiksnių atsitiktinio atsiradimo atveju. Determinuotais modeliais nustatomas tikslesnis rezultatas. Šie metodai taikomi esant nustatytiems rizikos veiksniams, kurie yra pastovūs, reguliarūs. Tuomet priimtų sprendimų pasekmės duoda tam tikrą rezultatą.

Vertinant galimas rizikos įgyvendinimo pasekmes, naudojamas imitacinio modeliavimo metodas. Imitacinius metodus sudaro rezultato rodiklių paieška daug kartų bandant modelį [32].

Vertinant kiekybines rizikas, naudojami jautrumo analizės ir imitavimo modeliavimo analitiniai metodai. Šie metodai naudojami nustatant kompleksinę organizacijos veiklos efektyvumą (atsparumą).

Jautrumo analizė numato nežymių rizikos veiksnių pokyčių įtaką rizikos vertinimo rezultatams. Jeigu nežymūs rizikos veiksnių pokyčiai sukelia nežymius rezultatų pokyčius, tuomet rizika yra maža. Taikant metodą, yra pašalinami visi rizikos veiksniai, išskyrus vieną. Tai yra pagrindinis metodo trūkumas, kadangi, vertinant riziką, neįmanoma gauti kompleksiško rezultato. Imitacijos procese kuriami nuoseklūs scenarijai naudojant modelio (neapibrėžtumo veiksnių) kintamuosius. Pagal šiuos duomenis daroma išvada apie galimų pasekmių lygį [33].

Kiekybinio vertinimo rezultatas – rodiklis. Kiekybinių rizikos rodiklių pavidalai pateikti Y paveiksle ir priklauso nuo to, ar pakanka turimos informacijos. Informacija analizei yra renkama iš skirtingų patikimų šaltinių. Vienas iš labiausiai patikimų informacijos šaltinių yra organizacijos vidaus ataskaitos, kurios prilygsta statistiniams informacijos šaltiniams.



4 pav. Rizikos vertinimo rodiklių sistema

Apibrėžtumo sąlygos nurodo informaciją apie analizuojamą objektą. Šiuo atveju dažniausiai naudojama normatyvinė dokumentacija: organizacijos vidaus ataskaitos, žiniaraščiai ir kiti patikimi rodikliai. Esant šioms sąlygoms, naudojami absoliutūs, santykiniai ir vidutiniai rodikliai. Absoliutūs rodikliai išreiškiami kainos arba turto vertės pavidalu. Santykiniai rodikliai palygina galimą žalą su esama baze. Šie rodikliai skaičiuojami naudojant koeficientus, orientuotus į rizikos įvykio pasekmes, arba į finansinius rodiklius (likvidumo koeficientus, mokumą, rentabilumą ir t.t.). Vidutiniai rodikliai naudojami apibendrinant rezultatus. Jie nurodo rizikų atsiradimo priežastis, rizikos veiksnius ir dėsningumą.

Esant dalinio neapibrėžtumo sąlygai, rizikos situaciją apibūdina rizikos įvykių atsiradimo dažnis. Šiuo atveju rizika vertinama kaip tikėtina. Vertinant kiekybinę riziką, taikomi tikimybės teorijos ir matematinės statistikos metodai. Tikimybiniai rodikliai – tai rizikos įvykio tikimybės ir pasekmių vertė. Naudojant šiuos rodiklius, svarbus tikimybinių reikšmių paskirstymo dėsnis. Statistiniai rodikliai charakterizuoja vidutinį tikėtinų veiklos reikšmių ir galimų nuokrypių vertę.

Visišką neapibrėžtumą sąlygoja informacijos apie rizikos situaciją trūkumas. Tuomet rizika vertinama remiantis ekspertinėmis žiniomis, formuojant individualius rizikos vertinimo rodiklius.

1.6. IT rizikos samprata ir standartai

Šiuolaikinės technologijos gali ne tik pagerinti procesų efektyvumą, bet ir sukelti didelę žalą, todėl IT rizika valdoma kaip tradicinė verslo rizika. IT rizikos sąvoka traktuojama įvairiai, priklausomai nuo standarto. Informacinių technologijų rizika, arba kibernetinė rizika, yra bet kokia su informacinėmis technologijomis susijusi rizika. Informacija vertinama kaip vertingas ir svarbus turtas, žinių, ekonomikos augimas ir skaitmeninė revoliucija nulėmė, kad organizacijos vis labiau priklauso nuo informacijos, jos apdorojimo ir informacinių technologijų priemonių.

ISO standartai apibūdina IT riziką kaip tam tikrą grėsmę pakenkti organizacijai, pasinaudojant turto ar turto grupės pažeidžiamumu. IT rizika vertinama pagal įvykio tikimybės ir jos pasekmių santykį [28].

Jungtinių Amerikos Valstijų nacionalinio saugos sistemų komitetas įvairiuose dokumentuose IT rizikos sąvoką traktuoja įvairiai.

2010 m. balandžio 26 d. Nacionalinio saugos sistemų komiteto (CNSS) instrukcijoje Nr. 4009 [34] pateikiamas toks techninio pobūdžio apibrėžimas: „Rizika – tai tam tikros grėsmės neigiamo poveikio IS galimybė, naudojanti ypatingą pažeidžiamumą“.

Nacionalinio saugumo telekomunikacijų ir informacinių sistemų saugumo instrukcijoje (NSTISSI) Nr. 1000 [35] įvedamas tikimybės aspektas, panašus į NIST SP 800-30: „Rizika – tai grėsmės tikimybės derinys, nurodantis grėsmės įvykio sukeltą neigiamą poveikį ir pasekmes“.

Nacionalinis informacijos užtikrinimo mokymo ir švietimo centras IT riziką įvardija kaip:

- nuostolių potencialą, atsirandantį dėl grėsmės pažeidžiamumo porų. Pavojaus sumažinimas arba pažeidžiamumas sumažina riziką;
- nuostolių netikrumą, išreikštą tokio nuostolio tikimybe;
- subjektui priešišką tam tikrą telekomunikacijų ar COMSEC sistemos išnaudojimą. Jos veiksniai yra grėsmė ir pažeidžiamumas;
- pavojaus tikimybės atsiradimą, kuris nurodo neigiamą grėsmės poveikį ir jo sukeltus sunkumus;
- tikimybę, kad tam tikra grėsmė paveiks sistemos pažeidžiamumą [17].

NIST leidiniuose IT rizikos apibrėžimas taip pat traktuojamas įvairiai.

Pagal NIST SP 800-30 rizika – tai tikimybė, kad tam tikras grėsmės šaltinis turi ypatingą galimą pažeidžiamumą, dėl kurio organizacijai daromas neigiamas poveikis [36].

Pagal NIST FIPS 200 rizika yra poveikio lygis organizacinėms operacijoms (įskaitant misiją, funkcijas, įvaizdį ar reputaciją), organizacijos turtui ar asmenims, atsirandantis dėl grėsmės ar jos tikimybės informacinei sistemai [37].

ISACA apibrėžia IT riziką kaip verslo riziką, susijusią su IT naudojimu, veikimu, įtaka įmonėje [38].

IT rizika turi platesnę reikšmę: ji apima ne tik neigiamą operacijų ir paslaugų teikimo poveikį, kuris gali sunaikinti ar sumažinti organizacijos vertę, bet ir naudą, suteikiančią galimybes naudoti technologijas. Tuomet IT naudojimas padeda išspręsti tokias problemas kaip didelės išlaidos arba pavėluotas pristatymas, turintis neigiamą poveikį verslui.

Informacinių sistemų rizikos valdymą sudaro rizikų identifikavimo, laipsnių vertinimo ir prevencijos priemonių taikymo procesai, siekiantys sumažinti riziką iki priimtino lygio. Galimybė laiku įvertinti riziką ir pritaikyti rizikos mažinimo prevencines priemones leidžia rasti tinkamą

apsaugos priemonių ir ekonominių sąnaudų balansą, užtikrinantį įmonės arba organizacijos veiklą, duomenų vientisumą ir apsaugą [36].

Vakarų šalių teisės aktuose reikalaujama, kad įmonės valdytų IT riziką. JAV to reikalauja „Sarbanes-Oxley“ įstatymas, priimtas 2002 m. Įmonėms privalomi informacinio saugumo standartai (pvz., ISO17799, BS7799, ISO27001) taip pat pateikia IT rizikos valdymo rekomendacijas ir metodus. IT rizikos įvertinimas leidžia bendrovei nustatyti išlaidų sumą, skirtą užtikrinti informacijos saugumą ir planuoti veiklą.

1.7. IT rizikos valdymo metodų apžvalga

Yra daug rizikos valdymo metodų, kurie atitinka kibernetinės saugos rizikos valdymo poreikius. Dauguma aprašyta ISO 31010 standarte. Kiekviena metodika turi privalumų ir trūkumų, deja, nėra aiškos sistemos, kurioje būtų nurodyta, kokių atveju reikėtų taikyti vieną ar kitą IT rizikos valdymo metodologiją. Daugumos organizacijų situaciją sunkina programinės įrangos, skirtos IT rizikai įvertinti ir valdyti, funkcionalumo apribojimai. Didelis programinės įrangos kiekis kuriamas nesivadovaujant IT rizikos valdymo metodologija ir informacijos saugumo standartais (pvz., BS7799 arba ISO17799), todėl netinkamai nustatomas ne tik IT rizikos lygis, bet ir atitikties laipsnis konkrečiam standartui.

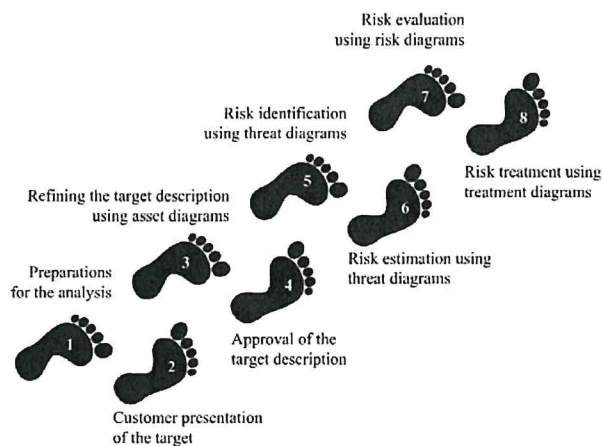
IT rizikos valdymo metodikų analizei parinktos trys IT standartus atitinkančios metodikos: CORAS, OCTAVE, CRAMM. Siekiant nustatyti metodikų trūkumus, yra palyginamas jų funkcionalumas ir atliekama SWOT analizė.

1.7.1. CORAS metodas

CORAS yra aiškiai apibūdinta knygoje „A Platform for Risk Analysis on Security Critical Systems — Model-based Risk Analysis Targeting Security“ [39]. Metodika buvo sukurta kaip „Information Society Technologies“ programos dalis. Jos esmė yra „Event-Tree-Analysis“, Markovo grandinės, „HazOp“ ir „FMECA“ [39] rizikos analizės metodų pritaikymas, tobulinimas ir derinimas. Metodikoje taikoma UML technologija. Ji yra pagrįsta Australijos/Naujosios Zelandijos standartu „AS/NZS 4360: 1999 Risk Management“ ir „ISO/IEC 17799-1: 2000 Code of Practice for Information Security Management“. Šiame standarte atsižvelgiama į rekomendacijas, pateiktas „ISO/IEC TR 13335-1: 2001 Guidelines for the Management of IT Security“ ir „IEC 61508: 2000 Functional Safety of Electrical/Electronic/Programmable Safety Related“.

Vadovaujantis CORAS, informacinės sistemos yra vertinamos ne tik kaip panaudotos technologijos, bet kaip sudėtingas kompleksas, kuriame yra atsižvelgiama į žmogiškuosius veiksnus. Šios metodikos taisyklės įgyvendinamos „Windows“ ir „Java“ programomis [40].

CORAS metodu saugumo rizikos analizę sudaro 8 etapai, kurie pavaizduoti 3 paveiksle.



5 pav. CORAS etapai

1 etapas – pasirengimas rizikos analizei. Etapo tikslas yra gauti tinkamą analizės apimties įvaizdį.

2 etapas – susitikimas su klientu. Etapo tikslas yra išdėstyti CORAS vertybes ir analizės tikslus.

3 etapas – tikslų aprašymo tobulinimas naudojant turto diagramas. Etapo tikslas yra supažinti su kliento poreikiais ir lūkesčiais. Apibrėžiamas tikslas ir taikymo sritis, nustatomas apsaugotinas turtas. Siekiant nustatyti pagrindinius grėsmės scenarijus, pažeidžiamumus ir įmonių lygio riziką tolimesniems etapams, atliekama apytikrė aukšto lygio analizė.

4 etapas – tikslinio aprašo patvirtinimas. Etapo tikslas – užtikrinti, kad likusios analizės pagrindiniai dokumentai, įskaitant tikslą ir apimtį, būtų teisingi, išsamūs ir atitiktų kliento poreikius. Prieš pradedant faktinę rizikos analizę, tikslo aprašymas yra patvirtinamas kliento. Šiame etape baigiamas konteksto kūrimas.

5 etapas – rizikos identifikavimas naudojant grėsmių diagramas. Etapo tikslas yra rizikos identifikavimas. Siekdama nustatyti riziką, CORAS naudoja struktūrizuotas idėjas. Struktūrizuotos idėjos – tai skirtingų kompetencijų analitikų seminaras, kuriame atliekama tikslų analizė. Privalumas yra tai, kad dalyviai turi skirtingas kompetencijas, todėl skirtingai vertina tikslą nei pavienė ar homogeninė grupė. Rizikos identifikavimas apima sistemingų grėsmių, nepageidaujamų incidentų, grėsmių scenarijų ir pažeidžiamumų nustatymą. Rezultatai, naudojant CORAS grėsmių diagramas, nedelsiant pateikiami.

6 etapas – pirminis rizikos vertinimas naudojant grėsmių diagramas. Etapo tikslas – nustatyti riziką, susijusią su nustatytais nepageidaujamais incidentais. Nepageidaujami incidentai buvo aprašyti grėsmių diagramose 5 etapo metu. Šios diagramos yra rizikos vertinimo pagrindas, kuriame įvertinamos nepageidaujamų incidentų tikimybės ir pasekmės. Rezultatai identifikuoja kiekvienos rizikos lygį. CORAS grėsmių diagramos palengvina tikimybių įvertinimą, argumentuojant vertinimo rezultatus tuo, kad esamos grėsmės sukelia nepageidaujamų incidentų.

7 etapas – pakartotinis rizikos vertinimas naudojant grėsmių diagramas. Etapo tikslas – nuspręsti, kokios rizikos yra priimtinos ir kokios turi būti pakartotinai vertinamos, siekiant jas sumažinti. Rizikos priimtumas identifikuojamas taikant nustatytus rizikos vertinimo kriterijus ir rizikos vertinimo rezultatus.

8 etapas – rizikos mažinimas naudojant mažinimo diagramas. Etapo tikslas – rizikos mažinimas ir analizė, ieškant rizikos mažinimo priemonių. Rizikos mažinimas padeda sumažinti nepageidaujamo incidento tikimybę ir pasekmes. Kadangi rizikų mažinimas gali būti brangus, prieš įgyvendinant galutinį rizikų mažinimo planą yra vertinamas sąnaudų ir naudos santykis.

1.7.2. OCTAVE metodas

OCTAVE apima aktyvų informacijos savininkų dalyvavimą nustatant kritinės informacijos turtą ir su tuo susijusią riziką. Metodas buvo sukurtas „Carnegie Mellon“ universiteto Programinės įrangos inžinerijos institute. Pagrindiniai OCTAVE elementai:

- kritinio informacijos turinio nustatymas;
- kritinio informacijos turto grėsmių nustatymas;
- pažeidžiamumų, susijusių su kritiniu informacijos turtu, nustatymas;
- rizikos vertinimas, susijęs su kritiniu informacijos turtu.

OCTAVE užtikrina didelį lankstumą, pasirenkant kriterijus, kuriuos įmonė gali naudoti taikydama metodiką savo poreikiams. Metodika skirta didelėms įmonėms, o jos populiarumas paskatino sukurti OCTAVE-S versiją mažoms įmonėms. Yra komercinių programinės įrangos produktų, įgyvendinančių OCTAVE nuostatas. Metodą sudaro 8 procesai, kurie išskaidyti į 3 etapus.

1 etapas – grėsmių profilių formavimas svarbios infrastruktūros atžvilgiu. Tikslas yra surinkti informaciją visoje organizacijoje ir nustatyti grėsmių profilius, svarbius organizacijos infrastruktūrai.

1 procesas – įmonės vadovybės žinių nustatymas. Analitikų grupė renka duomenis apie kritiškai svarbios infrastruktūros, saugumo reikalavimus, grėsmes, esamus organizacijos privalumus ir pažeidžiamumus, bendraudama su padalinių vadovais.

2 procesas – veiklos srities žinių nustatymas. Analitikų grupė renka duomenis apie kritiškai svarbios infrastruktūros, saugumo reikalavimus, grėsmes, esamus organizacijos privalumus ir pažeidžiamumus, bendraudama su analizuojamos veiklos srities specialistais.

3 procesas – operatyvinio personalo žinių nustatymas. Analitikų grupė renka duomenis apie kritiškai svarbios infrastruktūros, saugumo reikalavimus, grėsmes, esamus organizacijos privalumus ir pažeidžiamumus, bendraudama su operatyviuoju personalu ir IT specialistais.

4 procesas – grėsmių profilių formavimas. Analitikų grupė nustato nuo trijų iki penkių infrastruktūros vertybių ir formuoja grėsmių profilius.

2 etapas – infrastruktūros pažeidžiamumų nustatymas. Tikslas yra nustatyti svarbiausius sistemų komponentus, turinčius technologinių trūkumų ir pažeidžiamumų.

5 procesas – pagrindinių komponentų nustatymas. Analitikų grupė identifikuoja tipinius pagrindinius elementus, kurie padeda apdoroti organizacijai svarbią informaciją, sujungia juos į vieną rinkinį, nurodo vertinimo metodą.

6 procesas – pagrindinių komponentų įvertinimas. Analitikų grupė įvertina pasirinktus komponentus, rezultatus analizuoja, siekdama patobulinti kritinės infrastruktūros grėsmių profilius.

3 etapas – saugumo strategijos ir plano kūrimas. Tikslas yra įvertinti kritinės infrastruktūros riziką, parengti saugumo strategijos ir rizikos mažinimo planą.

7 procesas – rizikos analizė. Analitikai vertina kritinę organizacijos infrastruktūrą pagal nustatytus kriterijus ir išskaido rizikos profilius pagal rizikos sunkumo lygius (žema, vidutinė ir aukšta rizika). Rizikos vertinamos pagal jų poveikį kritinei infrastruktūrai. Tikimybė šiuo atveju nėra skaičiuojama, bet gali būti įtraukta į šį metodą.

8 procesas – apsaugos strategijos plėtra. Analitikų komanda rengia ir įgyvendina organizacijos saugos strategiją, orientuotą į rizikų sumažinimą ir kritinės infrastruktūros apsaugą.

1.7.3. CRAMM metodas

CRAMM metodą 1985 m. sukūrė Didžiosios Britanijos centrinės kompiuterių ir telekomunikacijų agentūros, ir jis buvo naudojamas tiek didelėms, tiek mažoms organizacijoms vyriausybiname ir komerciniame sektoriuose.

CRAMM apima technologijas, kurios grėsmes ir pažeidžiamumą įvertina, taikydamos netiesioginius veiksnius, be to, gali patikrinti rezultatus. Metodas turi informacinių sistemų saugumo perspektyvos modeliavimo mechanizmą, kuris naudoja išsamią atsakomųjų priemonių duomenų bazę. CRAMM vertina riziką ir efektyvumą taikydamas įvairių atsakomųjų priemonių derinį. Metodiką sudaro 10 procesų, kurie išskaidyti į tris etapus. Pirmo etapo metu aptariama saugumo

problema, antro etapo metu vertinama rizika ir trečio etapo metu parenkamos atsakomosios priemonės.

1 etapas – turto apimties vertinimas.

1 procesas – projekto rengimas. Saugumo konsultantas vykdo pasirinktų darbuotojų apklausą siekdamas gauti reikalingos informacijos. Organizuojamas posėdis, parengiama funkcinė specifikacija. Suderinamos projekto ribos ir surašomas fizinis (ryšio, aplinkos, programinės įrangos, techninė dokumentacija) ir duomenų (tarpusavyje susijusių) turtas. Užfiksuojama organizacijos struktūra ir duomenų naudotojai, nustatomi trys neprieinamumo laikotarpiai. Parengiamas projekto tvarkaraštis.

2 procesas – turto vertybių skirstymas. Fizinio turto vertybių skirstymas nėra sudėtingas, nes jo kaina yra žinoma. Sudėtinga įvardinti duomenų vertę. Duomenys skirtingu laikotarpiu turi skirtingą vertę. Siekdamas įvertinti duomenų vertę, konsultantas apklausia personalą. Pateikiamos anketos ir lentelės nurodant blogiausią atvejį. Svarbu, kad būtų ignoruojamos esamos atsakomybės priemonės ir personalas pateiktų tikslią bei reikšmingą skaitinę informaciją. Vertinant turtą, atsižvelgiama į politinio nesąžiningumo, asmeninio saugumo, asmens privatumo pažeidimo, teisinių įsipareigojimų nevykdymo, finansinių nuostolių, veiklos sutrikimų, komercinio konfidencialumo poveikį. Esant tam tikroms grėsmėms, šis poveikis gali tapti realybe (nuo mažų nuostolių iki įkalinimo ir viešo pažeminimo). Sukuriama duomenų turto suvestinė.

3 procesas – duomenų rezultatų patikra. Duomenys tikrinami tuo atveju, jei priskirtos vertės neatitinka realybės. Tai atsitinka, kai buvo apklaustas ne tos veiklos srities arba mažai žinių apie vertinamą turtą ir mažai patirties turintis personalas. Po to spausdinama CRAMM ataskaita, tuomet konsultantas rašo savo ataskaitą, kuri pateikiama organizacijos vadovybei. Organizacijoje aiškiai nurodoma konsultanto nuomonė apie kliento verslą. Suderinami turto vertinimai.

2 etapas – rizikos vertinimas.

4 procesas – nustatomi grėsmių poveikio santykiai. Šio etapo metu nustatomi reikšmingi grėsmių ir turto deriniai, jiems priskiriamas poveikis, skaičiuojami grėsmių poveikio santykiai.

5 procesas – įvertinamos grėsmės ir pažeidžiamumai. Grėsmių įvertinimas nustato grėsmių tikimybes. Įvertinimo metu atsižvelgiama į grėsmės įvykius praeityje ir organizacijos turtu susidomėjusius asmenis.

6 procesas – įvertinami saugos reikalavimai. Naudojama fiksuota trimatė paieškos lentelė (matrica). Reikšmes sudaro saugumo reikalavimai, surikiuoti pagal skirtingą grėsmių, pažeidžiamumų ir saugumo turto vertę.

7 procesas – saugos reikalavimų patikra. Siekiant išvengti nereikalingų išlaidų, dėl kurių gali atsirasti papildomas sistemų saugumo poreikis, yra tikrinamos saugos reikalavimų vertės. Riboto finansavimo atveju yra ieškoma kompromiso tarp rizikos ir išlaidų.

3 etapas – atitinkamų atsakomųjų priemonių parinkimas.

8 procesas – reikalingų atsakomųjų priemonių nustatymas. Parenkamų atsakomųjų priemonių rodiklis – tai apskaičiuoti saugos reikalavimai. CRAMM rinkinyje yra penkiasdešimt trys atsakomosios grupės, suskirstytos pagal galingumą (nuo 1 iki 5) į šiuos pogrupius: kaina; saugumo aspektas (techninė įranga, programinė įranga, ryšys, procedūros, fizinė sauga, personalas, aplinkosauga); paskirties tipas (grėsmės mažinimui, pažeidžiamumo mažinimui, poveikio mažinimui, aptikimui, atkūrimui).

9 procesas - atsakomųjų priemonių palyginimas. Parinktos priemonės lyginamos su jau įdiegtomis, siekiant nustatyti, kiek naujų atsakomųjų priemonių reikia įdiegti.

10 procesas – atsakomųjų priemonių patvirtinamas. Parinktos atsakomosios priemonės suderinamos su organizacijos vadovybe ir patvirtinamos.

IT rizikos valdymo sistemų charakteristikos pateiktos 1 priede, lentelėje Nr. 1. Duomenys išdėstomi pagal bendrą charakteristiką, įėjimo duomenų nustatymą, rizikos identifikavimą, valdymą, procesus, balanso skaičiavimą ir stebėjimą.

1.8. IT rizikos valdymo metodų SSGG analizė

Siekiant tiksliai nustatyti rizikos valdymo metodikų privalumus ir trūkumus, taikomas SSGG (Stiprybių silpnybių /galimybių grėsmių) analizės metodas. Remiantis 1 priede pateikta informacija, yra parenkamos svarbiausios rizikos valdymo metodikų charakteristikos, išvardintos 2 lentelėje.

2 lentelė. Rizikos valdymo metodikų SSGG charakteristikos

Charakteristikos
Perspėjimas dėl galimų rizikų
Autorinis palaikymas
Tinkamumas reguliariam taikymui
Investicijų grąžos skaičiavimas
Rizikos mažinimas
Techninio lygio rizikų vertinimas
Organizacinio lygio rizikų vertinimas
Likutinės rizikos valdymas
Rizikos prevencijos priemonių efektyvumo stebėjimas
Rizikos vertinimo rezultatų struktūrizuotas dokumentavimas
Reagavimas į IT incidentus
Pritaikymas skirtingo dydžio organizacijoms
Taikymo patogumas
Metodikos prieinamumas
Grėsmių bazė
Rizikos apėjimas
Rizikos priėmimas

Pagal išvardintas IT rizikos valdymo metodų charakteristikas atliekama SSGG analizė.

3 lentelė. CORAS metodikos SSGG

CORAS	
Stiprybės	Galimybės
Pritaikymas skirtingo dydžio organizacijoms	Perspėjimas dėl galimų rizikų
Taikymo patogumas	Autorinis palaikymas
Metodikos prieinamumas	Tinkamumas reguliariam taikymui
Rizikos priėmimas	Reagavimas į IT incidentus
	Rizikos mažinimas
	Techninio lygio rizikų vertinimas
	Organizacinio lygio rizikų vertinimas
	Rizikos vertinimo rezultatų struktūrizuotas dokumentavimas
Silpnybės	Grėsmės
Grėsmių bazė	Rizikos prevencijos priemonių efektyvumo stebėjimas
Rizikos apėjimas	Likutinės rizikos valdymas
	Investicijų grąžos skaičiavimas

CORAS metodikos SSGG analizės rezultatai pavaizduoti 3 lentelėje. Metodikoje nenumatytos darbuotojų informuotumo didinimo informacijos saugumo srityje, IT rizikos valdymo priemonės [41, 21]. Tokios priemonės gali sumažinti įmonės darbuotojų sukeltus informacijos saugumo režimo pažeidimus, perspėjant apie saugaus informacinių sistemų naudojimo reikalavimus. Be to, CORAS nenumato IT rizikos vertinimo dažnumo ir rezultatų atnaujinimo, tai rodo, kad metodika tinkama vienkartiniais vertinimams ir netinkama reguliariam naudojimui.

CORAS numatyta galimybė parengti rekomendacijas dėl rizikos mažinimo priemonių pasirinkimo, bet nėra galimybės įvertinti investicijų, įgyvendintų į saugumo priemones, efektyvumo. Taip pat nėra galimybės nustatyti tinkamo informacijos turinio nustatymo, taisymo ar atkūrimo prevencijos priemonių balanso. CORAS nenumato metodų veiksmingumo ir likutinės rizikos vertinimo būdų, tačiau jo privalumas yra tas, kad, naudojantis CORAS metodika, programinė įranga yra nemokama, ji nereikalauja didelių išteklių ją diegiant ir naudojant.

4 lentelė. OCTAVE metodikos SSGG

OCTAVE		
Stiprybės	Galimybės	
Pritaikymas skirtingo dydžio organizacijoms	Perspėjimas dėl galimų rizikų	
Taikymo patogumas	Autorinis palaikymas	
Metodikos prieinamumas	Investicijų grąžos skaičiavimas	
Rizikos priėmimas		
		Organizacinio lygio rizikų vertinimas
		Rizikos vertinimo rezultatų struktūrizuotas dokumentavimas
	Reagavimas į IT incidentus	
Silpnybės	Grėsmės	
Grėsmių bazė	Rizikos mažinimas	
Rizikos apėjimas	Techninio lygio rizikų vertinimas	
Rizikos prevencijos priemonių efektyvumo stebėjimas	Likutinės rizikos valdymas	
	Tinkamumas reguliariam taikymui	

Nepaisant to, kad OCTAVE metodika atitinka rizikos kriterijus, rizikų stebėjimas yra jos silpnoji dalis [42, 43]. OCTAVE numato reguliarių IT rizikos vertinimą ir rezultatų atnaujinimą. Nustatant rizikos valdymo strategiją, OCTAVE daro prielaidą, kad rizikų mažinimo priemonė naudojama tik rizikoms sumažinti ir priimti. Šis rizikos valdymo apėjimo (išimties) būdas nenaudojamas.

OCTAVE metodika pritaikoma konkrečioms sąlygoms, pavyzdžiui, įmonės dydžio, verslo rūšies, teisės aktų bei tam tikrų standartų reikalavimams ir kt. OCTAVE nepateikia kiekybinio rizikos įvertinimo, tačiau kokybinis vertinimas gali būti naudojamas nustatant reitingavimo mastą. Įvertinimas gali apimti įvairias rizikos sritis, kurios nėra tiesiogiai įtrauktos į metodiką, išskyrus technines rizikas ir įstatymų pažeidimo riziką, kadangi į jas netiesiogiai atsižvelgiama tik informacijos turto savininkų apklausos metu. Tuomet paaiškėja, kokios pasekmės gali kilti grėsmės atveju. Metodika nesuteikia aiškaus nurodymo, kaip pastebėti pavojų, tačiau pabrėžia rizikos dėl pavojaus egzistavimo svarbą. OCTAVE metodika atitinka rizikos mažinimo priemonių veiksmingumo vertinimo ir struktūrizuoto požiūrio į rizikos valdymą reikalavimus.

5 lentelė. CRAMM metodikos SSGG

CRAMM	
Stiprybės	Galimybės
Pritaikymas skirtingo dydžio organizacijoms	Perspėjimas dėl galimų rizikų
Taikymo patogumas	Tinkamumas reguliariam taikymui
Grėsmių bazė	Rizikos mažinimas
Rizikos apėjimas	Techninio lygio rizikų vertinimas
Rizikos priėmimas	Organizacinio lygio rizikų vertinimas
Silpnybės	Grėsmės
Metodikos prieinamumas	Autorinis palaikymas
	Likutinės rizikos valdymas
	Rizikos prevencijos priemonių efektyvumo stebėjimas
	Rizikos vertinimo rezultatų struktūrizuotas dokumentavimas
	Reagavimas į IT incidentus
	Investicijų grąžos skaičiavimas

Metodikoje visiškai neatsižvelgiama į darbuotojų informuotumą informacijos saugumo srityje, patvirtinamuosius dokumentus, pvz., verslo procesų aprašymą arba atliktų IT rizikos vertinimų ataskaitas [44]. CRAMM apima tik rizikų mažinimo metodus. Rizikos valdymo metodai, pvz., vengimas ar priėmimas nėra priimtini.

Rizikos elementų nustatymas yra stiprioji metodikos dalis. Nustatomi tokie rizikos elementai kaip materialusis ir nematerialusis turtas, vertė, grėsmės, saugumo priemonės, galimos žalos ir grėsmės tikimybė. CRAMM metodika naudoja kiekybinius ir kokybinius IT rizikos įvertinimo metodus, tačiau neturi apibrėžtų sąlygų, kuriomis įmonės gali remtis. Rizikos valdymo metodikos priemonės taikymo sprendimai turi būti grindžiami ne tik rizikos dydžiu, bet įgyvendinimo ir

nuosavybės sąnaudomis. CRAMM neapima investicijų grąžos apskaičiavimo įgyvendinant saugumo priemonės. CRAMM metodika turi didelių trūkumų. Joje nenumatyta:

- kontrolės metodų integravimas;
- konkretaus metodo tikslo aprašymas;
- taikomų valdymo metodų veiksmingumo stebėjimas;
- likutinės rizikos valdymo metodai;
- didžiausių leistinų rizikos verčių perskaičiavimas;
- reagavimo į incidentus procesai.

Praktinis CRAMM taikymas reikalauja sudėtingo ir kruopštaus aukštos kvalifikacijos specialistų darbo apdorojant CRAMM programine įranga sugeneruotus ataskaitų dokumentus, turinčius šimtus tūkstančių puslapių.

2. IT rizikos valdymo metodo tobulinimo sprendimai

Rizikos valdymas – svarbi organizacijos strategijos planavimo dalis. Egzistuoja daug įvairių rizikos valdymo metodų. Svarbiausiai metodų procesas – rizikos vertinimas. Apžvelgtuose metoduose (CORAS, OCTAVE, CRAMM) rizika vertinama turto vertės nustatymo ir scenarijų analizės principu. Organizacijos turto vertė kinta pastoviai ir atsekti bei numatyti tikrą jos dinamiką yra sudėtinga.

Matematinio modelio rizikos vertinimo metodai (BS 7799, KURAP, KRA, TMN, Atakos medžio metodas), kuriuose rizika vertinama taikant tikimybių, pažeidžiamumų ir žalos santykius tinka verslo procesams ir sunkiai adaptuojasi informacinių technologijų ir kibernetinės saugos procesams.

Scenarijų analizės metodai padeda tiksliai nustatyti galimus įrangos sutrikimus, kadangi šiuos sutrikimus sukeliantys veiksmai yra iš anksto žinomi ir tam tikrų požymių įgyvendinimo scenarijai leidžia nustatyti atitinkamus rezultatus, kuriais operuojant vertinama rizika. Vertinant žmogaus poveikio riziką, metodas yra neefektyvus, kadangi numatyti žmogaus veiksmus yra sudėtinga. Atitinkamai rizikos rezultatų tikslumą nustatyti sudėtinga.

Matematinio modelio rizikos vertinimo metodai reikalauja patobulinimų, kadangi kiekvienai organizacijai taikomi individualūs rizikos tikimybių vertinimo kriterijai, kurių dydis nustatomas pagal individualų organizacijos poreikį, todėl yra sudėtinga lyginti atskirų organizacijų rizikos vertinimo rezultatus, siekiant nustatyti rizikos tendencijas. Kadangi organizacijose gali būti taikomos įvairaus sudėtingumo lygio informacinės sistemos, bet kurio metu gali atsirasti nauji pažeidžiamumai, kuriuos numatyti yra taip pat sudėtinga, tai lemia netikslus su informacinėmis technologijomis susijusios rizikos rezultatus. Analizuotų rizikos vertinimo metodų ir kitų metodų rezultatai išreiškiami galimais piniginiiais nuostoliais. Techninių rizikų vertinimui skiriama mažai dėmesio ir nėra objektyvių rizikos vertinimo aprašymų. Kadangi techninės rizikos nereikalauja labai aukšto matematinio tikslumo, o svarbus yra rizikos egzistavimo faktas ir esamo fakto mastas, reikalingas metodas, kuris akivaizdžiai parodytų IT rizikos rezultatus. Dėl šių priežasčių, siekiant įvertinti riziką balo metodu, būtinas balo metodo performavimas.

2.1. Siūlomo metodo tikslas ir reikalavimai

Patobulinti matematinio modelio analitinį rizikos vertinimo metodą, kuomet rizikos vertinimo rodikliai yra nustatomi vertinimo objekto informacijos apibrėžtumo atveju, naudojant bendrus rodiklių nustatymo kriterijus, kurių naudojimas leidžia taikyti metodą skirtingoms organizacijoms. Rezultatų segmentavimas leis greitai ir lengvai įvertinti techninių IT rizikų rodiklius, o rizikų rezultatus išreikšti keturių segmentų skalėje (žemas, vidutinis, aukštas, labai aukštas rizikos lygis). Metodas turi atitikti šiuos reikalavimus:

- rizikos vertinimas turi būti vykdomas grėsmės realizavimo tikimybės ir galimos žalos lygio santykio pagrindu, kuomet apibrėžtus duomenys sudaro įmonėje atliktas auditas, o grėsmių ir pažeidžiamumų kiekis nustatomas įvertinant galimus scenarijus pagal ISO/ IEC 27005 aprašą;
- grėsmės realizavimo tikimybės ir galimos žalos lygio santykių kriterijai turi būti pritaikomi skirtingoms organizacijoms, kuriuose yra naudojama IT infrastruktūra. objektyvius organizacijos technines IT rizikos veiksnius susijusius su informacinių technologijų infrastruktūros veikimo tęstinumu, turinčio įtaką organizacijos veiklos įsipareigojimų įgyvendinimui, dėl kurių sutrikimo organizacija gali patirti bet kokio pobūdžio žalą;
- informacinių technologijų infrastruktūros rizikos vertinimo procesas, turi būti įgyvendintas taikant klasikinę rizikos vertinimo formulę;
- numatyti galimybę keičiantis vidaus arba išorės rizikos veiksniams (informacinės technologijos, kibernetinės grėsmės, pažeidžiamumai, personalas) stebėti rizikos jautrumą;
- metodas turi būti palankus naudotojams ir nereikalausti specifinių, arba matematinių žinių, siekiant gauti vertinimo rezultatus.

2.2. Siūlomo metodo sprendimai

Modelio formavimas paremtas klasikinę rizikos vertinimo formulę. Kibernetinių rizikų klasikinę formulę sudaro trijų kintamųjų funkcija:

- Grėsmės tikimybė
- Pažeidžiamumo tikimybė
- Potenciali įtaka

Bet kuriam išvardintam kintamajam prilyginant nuliui, rizika prilygsta nuliui. Vadovaujantis ISO/IEC 27001 standarto IT saugos aprūpinimo metodų reikalavimais, metodas privalo garantuoti palyginamus ir atkartojamus rezultatus. Standarte nepateikta skaičiavimo formulė. NIST 800-30 standarte „Risk management guide for information technology systems“ pateikta šia IT rizikos vertinimo formulė:

$$R = P(t) * S \quad [1]$$

Kur: R – rizikos vertė;

P(t) – kibernetinių grėsmių realizavimo tikimybė;

S – Turto vertė

Pagal LST ISO/IEC 13335-3:2000 standartą „Information technology. Security techniques. Part 3. Techniques for the management of information technology security“ IT rizika vertinama taikant šią formulę:

$$R = P(t) * P(v) * S \quad [2]$$

Kur: R – rizikos vertė;

P(t) – kibernetinių grėsmių realizavimo tikimybė;

P(v) – Pažeidžiamumo išnaudojimo tikimybė;

S – turto vertė.

Šiuo atveju P(t) ir P(v) tikimybių reikšmės išreiškiamos trijų lygių kokybės skalėje (žema, vidutinė, aukšta). „S“ reikšmės intervalas kinta nuo 0 iki 4. Kokybinio rodiklio atitiktį nustato organizacija, kurioje vykdomas IT rizikos vertinimas.

Pagal BS 7799-2:2005 standartą „Code of practice for information Security Management“ rizika vertinama atsižvelgiant į turto vertės rodiklį, grėsmes, ir pažeidžiamumo lygį, pagal šią formulę:

$$R = S * L(t) * L(v) \quad [3]$$

Kur: R – rizikos vertė;

S – turto vertė;

L(t) – grėsmės lygis;

L(v) – pažeidžiamumo lygis.

Rizikos vertinimo žingsniai pateikti 5 lentelėje. Remiantis gautų rezultatų analizę, atrenkami rizikos veiksniai turintys aukščiausią įgyvendinimo tikimybę ir nustatomos atsakomosios priemonės, kurių pagalba yra mažinama rizika. Skaičiuojama IT rizikos veiksmų dinamikos tendencija, atliekamas pakartotinis rizikos vertinimas ir analizuojami rezultatai. Apie kiekvieną žingsnį pateikiama platesnė informacija.

6 lentelė. Siūlomo rizikos valdymo metodo sprendimai

Žingsniai	Priemonės
1. IT rizikos apimties nustatymas	Pokalbis su aukščiausio lygio vadovais ir teisininkais, organizacijos charakteristikos formavimas. Rizikos ir duomenų kategorijos nustatymas
2. Organizacijos techninės dokumentacijos analizė	Organizacijos dokumentacijos analizė
3. Pažeidžiamumų ir grėsmių nustatymas	ISO/IEC 27005 Priedas C „Tipinių grėsmių pavyzdžiai“, Priedas D „Pažeidžiamumai ir jų vertinimo metodai“ (pateikti šio darbo 2 ir 3 prieduose). Rizikų skirstymas pagal kategorijas.

4. Personalo apklausa	Apklauso anketa ir vertinimo metodika (pateikti šio darbo 6 ir 7 prieduose)
5. Galimo žalos lygio, grėsmių realizavimo tikimybės ir rizikų įvertinimas	NIST 800-30 standarto formulė $R = P(t) * S$;
6. Rizikos rezultatų reitingavimas ir segmentavimas	Pagal nustatytus kriterijus
7. Rizikos mažinimas	Taikomi rizikos mažinimo techniniai sprendimai.
8. Rizikos jautrumo analizė	pakartotinis įvertinimas, siekiant nustatyti dinamikos tendenciją.

1 žingsnis – IT rizikos apimties nustatymas. Vykdoma organizacijos aukščiausio lygio vadovo ir teisininko apklausa, nustatomi organizacijos IT rizikos vertinimo poreikiai. Siekiant nustatyti IT infrastruktūros reikalavimus, formuojama įmonės charakteristika, kurios pagrindu nustatomos objektyvios organizacijos rizikos ir jų priklausomybė nuo duomenų kategorijos.

2 žingsnis – Organizacijos techninės dokumentacijos analizė. Analizuojama organizacijos IT tvarka ir saugos reikalavimai, atsižvelgiant į šiuos reikalavimus:

- Tapatumo patvirtinimas;
- Vartotojų ir administratorių auditas ir kontrolė;
- Įsibrovimo aptikimas ir prevencija;
- Belaidžio tinklo saugumas ir kontrolė;
- Svetainių, pasiekiamų iš viešųjų elektroninių ryšių tinklų, saugumas ir kontrolė.

3 žingsnis – Pažeidžiamumų ir grėsmių nustatymas. Remiantis technines dokumentacijos analize, nustatomi pažeidžiamumai grėsmės, išvardinti šio darbo 3 priede. Duomenų nustatymui, naudojamas matematinio modelio analitinis metodas, esant pilnam duomenų neapibrėžtumui, kuomet duomenų nustatymui taikomos ekspertinės žinios, analizuojant ir užpildant duomenų lenteles pateiktas 4 ir 5 šio darbo priede.

4 žingsnis – Personalo apklausa. Remiantis atlikta analize yra formuojama apklauso anketa, kuri bus dalinama IT infrastruktūros techninio palaikymo specialistams. Anketos pagalba yra įvertinami pažeidžiamumo išnaudojimo asmenų potencialas, taikomų prevencijos priemonių efektyvumas, informacinių sistemų kritiškumas, procesų pažeidžiamumo lygis, organizacijos veiklos reguliavimas ir reputacijos lygis. Klausimai sudaryti „pasirinkimo“ principu, kuomet apklausomas asmuo gali pasirinkti tik alternatyvas. Toks būdas padeda gauti objektyvius atsakymo rezultatus, padeda nustatyti reikiamus duomenys ir išvengti asmeninės nuomonės, siekiant nustatyti grėsmės realizavimo tikimybę ir galimos žalos lygį. Apklauso anketa ir rezultatų įvertinimo metodika pateikta šio darbo 6 priede.

5 žingsnis – Galimo žalos lygio ir grėsmių realizavimo tikimybės įvertinimas. Kiek vienos rizikos galimi nuostoliai išreiškiami balais nuo 0,25 (maži nuostoliai) iki 1 (dideli nuostoliai). Kriterijai pateikti 6 lentelėje. Įvertinimas vyksta dalyvaujant atitinkamų kvalifikacijų specialistams, pagal šias veiksmų kategorijas:

- Duomenų kategorija;
- Informacinės sistemos kritiškumui;
- Procesų pažeidžiamumo lygis;
- Organizacijos veiklos reguliavimas;
- Reputacijos lygis.

7 lentelė. Galimo nuostolių lygio kriterijai (pavyzdys)

Duomenų kategorija	Informacinės sistemos kritiškumams	Procesų pažeidžiamumo lygis	Organizacijos veiklos reguliavimas	Reputacijos lygis	Galimas nuostolių lygis (S)
Komercinė paslaptis	Labai kritinė	Kelių procesų sutrikimai, veiklos sustojimas	Neplaninės komisijos patikros, baudos	Reputacija pažeminama tautiniame lygyje	Labai aukštas
Gamybinė paslaptis	Kritinė	Proceso sutrikimai	Auditai, padidintas dėmesis	Reputacija pažeminama regioniniame lygyje	Aukštas
Tarnybinė informacija	Iš dalies kritinė	Proceso greičio sumažinimas	Nurodymai be baudų ir auditų	Reputacija pažeminama internetu	Vidutinis
Atvira informacija	Ne kritinė	Nėra įtakos	Nėra jokių nurodymų	Reputacija nepažeminama	Mažas

Grėsmės realizavimo tikimybė skaičiuojama remiantis ISO/IEC 27005 standarto „C“ ir „D“ priedų duomenimis. Suformuojama skalė, kriterijai pateikti 7 lentelėje, kur reikšmių diapazonas kiekvienam kriterijui yra nuo 0,25 (maža grėsmės realizavimo tikimybė) iki 1 (labai aukšta grėsmės realizavimo tikimybė). Suminė grėsmių realizavimo tikimybė lygi 4 balams. Įvertinimas taip pat vyksta dalyvaujant atitinkamų kvalifikacijų specialistams, pagal šias veiksmų kategorijas:

- Aktyvių grėsmių kiekis atitinkamai rizikai
- Pažeidžiamumų kiekis atitinkamai rizikai
- Grėsmės arba pažeidžiamumo išnaudojimo asmenų potencialas
- Taikomų prevencijos priemonių lygis

8 lentelė. Grėsmių realizavimo tikimybės kriterijai (pavyzdys)

Aktyvių grėsmių kiekis (T-Threats)	Pažeidžiamumų kiekis (A-Assets)	Grėsmės arba pažeidžiamumo išnaudojimo asmenų potencialas	Taikomų prevencijos priemonių efektyvumas	Grėsmės realizavimo tikimybė P(t)
75%-100% (Tmax)	75%-100% (Amax)	Administratorius	Žemas	Labai aukšta incidento tikimybė
50%-75% (Tmax)	50%-75% (Amax)	Kiti darbuotojai	Vidutinis	Aukšta incidento tikimybė
25%-50% (Tmax)	25%-50% (Amax)	Buvusieji darbuotojai; Programinės įrangos kūrėjai.	Aukštas	Vidutinė incidento tikimybė
25% (Tmax) < = 1 grėsmė	25% (Amax) < = 1 grėsmė	Nekvalifikuoti asmenys	Labai aukštas	Žema incidento tikimybė

Nustatytų grėsmių kiekis išreiškiamas kintamuoju „n“, kuris proporcingai kinta grėsmės realizavimo tikimybės P(t) atžvilgiu. Pažeidžiamumų kiekis išreiškiamas kintamuoju „i“. Atitinkamai grėsmių kiekiui, pažeidžiamumai kinta proporcingai P(t) reikšmei. Grėsmių ir pažeidžiamumų reikšmės apvalinamos iki sveiko skaičiaus, taikant standartinį apvalinimo metodą. Formuojamam metodui taikoma [1] formulė.

6 žingsnis – Rizikos rezultatų reitingavimas ir segmentavimas. Rezultatų reitingavimo skalė pateikta 4 paveiksle. Gauti vertinimo rezultatai paverčiami procentinę išraišką ir reitinguojami pagal 20 balų santykį, segmentuotus į 4 grupes:

- I grupė – žema rizika (nuo 0 iki 5 balų);
- II grupė – vidutinė rizika (nuo 6 iki 10 balų);
- III grupė – aukšta rizika (nuo 11 iki 15 balų);
- IV grupė – labai aukšta rizika (nuo 16 iki 20 balų).

Rizikos	žema	vidutinė	aukšta	labai aukšta
R	0-5 balų 25%	6-10 balų 50%	11-15 balų 75%	16-20 balų 100%

6 pav. Rizikos rezultatų reitingavimo skalė

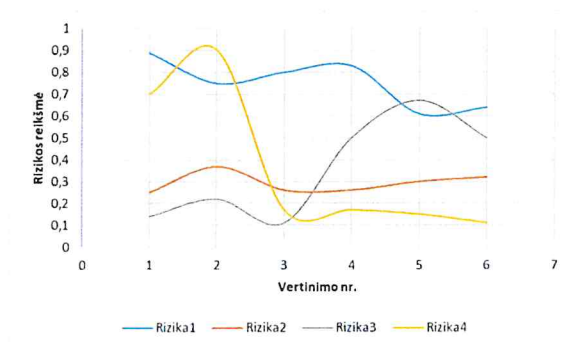
7 žingsnis – Rizikos mažinimas. Atlikus rizikos vertinimo žingsnį, nustatomos organizacijos IT infrastruktūros trūkumai. Pildoma atsakomųjų priemonių nustatymo forma, kurios pavyzdys pateiktas 5 paveiksle. Stulpelyje „Pažeidžiamumas“ surašomi IT infrastruktūros silpnos vietos. Stulpelyje „pažeidžiamumo šaltinis“ surašomos trūkumų atsiradimo priežastys. Tam kad nustatyti pažeidžiamumo šaltinį, yra atliekama organizacijos vidaus ekspertizė, apklausomi atsakingi asmenys,

kol išaiškės pažeidžiamumo šaltinis. Stulpelyje „atsakomosios priemonės“ surašomos galimos pažeidžiamumų išnaudojimo prevencijos priemonės. Užpildyta forma pateikta 6 priede. Užpildžius formą, organizacijoje vykdoma rizikos prevencijos intervencija, kurios metu yra taikomos nustatytos atsakomosios priemonės. Pritaikius atsakomąsias priemones būtinas pakartotinis rizikų vertinimas.

Nr.	Pažeidžiamumas	Pažeidžiamumo šaltinis	Atsakomosios priemonės
1.	Darbuotojams paliekant darbo vietą, neužsiblokuoja ekranas	Neįjungta ekrano blokavimo funkcija	Įjungti ekrano blokavimo funkciją
...	...	...	...
...	...	...	...

7 pav. Atsakomųjų priemonių nustatymo forma (pavyzdys)

8 žingsnis – Rizikos jautrumo analizė. Rizikos vertinimo duomenys pavaizduojami grafiškai nenutrūkstamoje skalėje. Grafiko pavyzdys pateikiamas 6 paveiksle. Toks sprendimas leidžia stebėti rizikų dinamiką siekiant sumažinti riziką, arba atlikus pakartotinį vertinimą po tam tikro laikotarpio. Sprendimas taip pat identifikuoja rizikos pokyčio priklausomybę nuo rizikos tikimybės rodiklių pokyčio.



8 pav. Rizikų dinamikos grafikas (pavyzdys)

Jautrumo analizei parenkamos rizikos turinčioms didžiausią reikšmę, kurioms nustatomos pažeidžiamumų ir grėsmių pokyčių sąlygos, pagal kurias yra vertinama pažeidžiamumų ir grėsmių įtaka rizikos rezultatui.

3. Patobulinto IT rizikos valdymo metodo praktinis taikymas

Metodo praktinis pritaikymas vykdomas pagal pasiūlytus rizikos valdymo metodo žingsnius. Duomenys šiame skyriuje yra pakoreguoti pateiktos informacijos konfidencialumo tikslais.

3.1. IT rizikos apimtys nustatymas

P Duomenys surenkami vykdant pokalbį su aukščiausio lygio vadovais ir įmonės juristais.

„Įmonė A“ – energetikos įmonė, kurios veiklos sritis – karšto ir geriamo vandens tiekimas, geriamo vandens gavyba, šilumos gamyba ir nuotekų tvarkymas. Dėl plataus veiklos spektro įmonės veikla išskaidyta į 11 padalinių:

- Administravimo padalinys
- Išteklių tiekimo padalinys
- Buhalterijos padalinys
- Energijos tiekimo padalinys
- Gamybos padalinys
- Klientų aptarnavimo padalinys
- Valymo įrangos padalinys
- Vandens gavybos padalinys
- Cheminių tyrimų padalinys
- Vandens ir nuotekų tinklų aptarnavimo padalinys
- Šilumos gamybos padalinys

Įmonėje dirba 200 žmonių, iš kurių 90 darbuotojų turi kompiuterizuotą darbo vietą. Įmonės informacinės sistemos veikia keturių fizinių serverių pagrindu, kuriuose įdiegta 10 virtualių serverių. Serveriai yra išdėstyti visos įmonės teritorijose, atstumas tarp kurių viršija 20 km. Iš viso yra keturios serverinės, kuriuose yra įrengtos nepertraukiamo maitinimo ir mikroklimato valdymo sistemos. IT infrastruktūra komutuojama optinio ryšio kabeliu. Vidaus tinklo greitis – 1Gbps. Siekiant sumažinti tinklo infrastruktūros sutrikimų kiekį, optinio kabelio sujungimui naudojami tik SFP moduliai. Tinklo įranga yra unifikuota (visoje įmonėje naudojami vieno modelio, skirtingų portų kiekio valdomi komutatoriai), kurie turi „Life time“ gamyklinę garantiją. Esant tinklo įrangos gedimui, yra numatytos „ZIP“ atsargos, kurias sudaro kiekvieno komutatoriaus tipo 1 atsarginis įrenginys. Ugniasienės ir pagrindiniai komutatoriai dirba „Active-Passive“ klasteryje. Tai užtikrina tinklo saugos tęstinumą ir

išorės interneto prieinamumą. IT infrastruktūra pakurta Microsoft sprendimų pagrindu. Iš viso naudojama 100 vnt. licencijuotų operacinių sistemų iš kurių:

- 48% – Windows 10 Professional;
- 15% – Windows 8.1 Home and Business;
- 5% – Windows 7 Professional;
- 22 vnt. – Windows XP Professional.

3.1.1. IT infrastruktūros pagalba vykdomi šie įmonės procesai

Gamybiniai procesai. Įmonė valdo šilumos gamybos, geriamo vandens gavybos ir nuotekų tvarkymo gamybinius procesus. IT infrastruktūra priskirta kritinės infrastruktūros grupei ir naudojama nuotoliniam gamybinės įrangos valdymui ir gamybinių procesų stebėjimui. Gamybinė IT infrastruktūra izoliuota nuo bendrai naudojamo kompiuterinio tinklo ir veikia atskirame vidiniame tinkle, kurio veikimui naudojama atskira tinklo įranga. Esant šio proceso IT infrastruktūros sutrikimams, numatyta galimybė valdyti ir stebėti gamybinę įrangą rankiniu būdu. Šiuo atveju kibernetinės grėsmės neturi didelės įtakos gamybinių procesų technologijai.

Laboratoriniai procesai. Įmonėje įrengta chemijos ir bakteriologijos tyrimų laboratorija, kuri tiria geriamojo vandens, kietojo kuro ir nuotekų mėginius ir priklausomai nuo tyrimų rezultatų teikia pastabas, arba rekomendacijas atitinkamiems gamybiniams procesams. IT infrastruktūra priskiriama prie svarbios infrastruktūros ir naudojama tyrimo rezultatų duomenų įvedimui į registrus, saugojimui ir ataskaitų ruošimui valdybai, valstybės kontrolės komisijai ir auditui. Duomenys yra priskiriami prie gamybinės paslapties kategorijos ir jų praradimas, arba suklastojimas gali neigiamai įtakoti tolimesniąją laboratorijos veiklą. Siekiant sumažinti kibernetinių grėsmių riziką, duomenų kopijos yra nukreiptos į failų saugojimo serverį, prieiga prie šių duomenų yra suteikta tik asmenims turintiems teisę disponuoti šiais duomenimis.

Paslaugų tiekimo procesai. Įmonė vykdo šilumos, karšto ir geriamo vandens tiekimą. IT infrastruktūra priskirta vidutinės svarbos grupei ir atlieka tik galutini produktą teikiančios įrangos parametrų stebėjimo funkciją. Įrangos valdymas vykdomas rankiniu būdu ir IT infrastruktūros sutrikimai nesustabdo paslaugų tiekimo technologijos. Duomenys priskiriami prie tarnybinės informacijos kategorijos.

Klientų aptarnavimo procesai. Įmonė teikdama paslaugas, vykdo šiuos aptarnavimo procesus: registruoja avarinių situacijų pranešimus, tikrina ir keičia šalto ir karšto vandens skaitiklius, suteikia konsultacinę pagalbą, vykdo atsiskaitymo už paslaugas funkciją. Klientai – prioritetinis dalykas. IT infrastruktūra priskirta labai kritinės infrastruktūros grupei. Duomenys priskirti komercijos paslapties kategorijos. Sutrikimai šiuo atveju gali sukelti klientų aptarnavimo procesų

tęstinumo pažeidimą ir asmens duomenų nutekėjimą. Pasekmės – įmonės įvaizdžio ir reputacijos pažeminimas.

Vidaus resursų ir išteklių valdymo procesai. Įmonės veiklą sudaro Atsargų ir gamybos, finansų apskaitos ir personalo valdymo procesai. IT infrastruktūra priskirta labai kritinės infrastruktūros grupei. Duomenys priskirti komercijos paslapties kategorijos. Visos sistemos veikia vienoje platformoje. IT infrastruktūros sutrikimai sukelia valdymo procesų pažeidimus, dėl kurių įmonė negali laiku vykdyti veiklos įsipareigojimus. Atsiranda mokestinės prievolės ir kita žala.

Ryšių su visuomenę procesai. Įmonė nuolat palaiko ryšį su visuomenę, teikia informacija žiniasklaidai, rengia seminarus ir konferencijas, skelbia konkursus ir kt. IT infrastruktūra priskirta žemos svarbos kategorijai ir jos sutrikimai neturi įtakos įmonės veiklai. Duomenys yra atviri visiems ir jų išskleidimas taip pat neturi jokios įtakos įmonės procesų veikimui.

3.2. Organizacijos techninės dokumentacijos analizė

Įmonės IT infrastruktūros dokumentacija parengta vadovaujantis Lietuvos Respublikos vyriausybės nutarimu „dėl bendrųjų elektroninės informacijos saugos reikalavimų aprašo, saugos dokumentų turinio gairių aprašo ir elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo“, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu ir Lietuvos Respublikos aplinkos ministro įsakymu „dėl nacionaliniam saugumui užtikrinti svarbių vandens tiekimo ir nuotekų šalinimo paslaugas teikiančių įmonių fizinės ir informacinės saugos reikalavimų patvirtinimo“. Įmonėje yra patvirtinti ir galiojantys šie dokumentai:

- informacinių sistemų fizinės saugos tvarka. Ji apibūdina pateikimo į įmonės serverines tvarką, kurioje nurodomas asmenų, galinčių patekti į ryšio ir serverių patalpas, sąrašas;
- kibernetinės saugos politika. Dokumentas nusako standartus, vadovaujantis kuriais yra užtikrinamas kibernetinis saugumas įmonėje. Įmonė vadovaujasi ISO/IEC 27000 serijos standartais;
- informacinių sistemų duomenų saugos tvarka. Dokumente aprašomos duomenų konfidencialumo ir IS infrastruktūros svarbos kategorijos. Išsami informacija pateikta nustatytų rizikų 8 lentelėje;
- naudojimosi kompiuterių sistemomis taisyklės. Dokumente aprašomi naudojimosi įmonės IT infrastruktūra reikalavimai (kompiuterinio tinklo, kompiuterinių sistemų, programinės įrangos naudojimas), slaptažodžių keitimosi politika ir tvarka, darbo vietos priežiūros tvarka, atsakomybės.

3.2.1. Dokumentuose apibrėžti reikalavimai

Tapatumo patvirtinimas:

- kompiuterinių sistemų (toliau - KS) administravimui naudojamos tam skirtos paskyros;
- KS vartotojams nesuteikiamos administratoriaus teisės;
- viešuoju tinklu perduodama informacija yra konfidenciali ir šifruojama;
- kiekvienas KS vartotojas patvirtina savo tapatybę autorizacijos būdu;
- baigus darbą arba pasitraukiant nuo KS vartotojai atsijungia nuo darbo paskyros, įjungiamo ekrano užsklanda su slaptažodžiu;
- vartotojui neatliekant KS jokių veiksmų, darbo paskyra užrakinama. Toliau dirbti galima tik parkartotinai patvirtinus vartotojo tapatybę;
- vykdoma KS vartotojų administravimo paskyrų kontrolė;
- techninėje ir programinėje įrangoje nenaudojami gamintoju nustatyti slaptažodžiai. Visi slaptažodžiai yra pakeisti ir atitinka reikalavimus.

KS vartotojų ir KS administratorių atliekamų veiksmų auditas ir kontrolė:

- KS yra fiksuojama įvykių informacija, remiantis kuria yra atsiejami vartotojų veiksmai ir kibernetinės saugos incidentai;
- Audituojamų duomenų laiko žymos sinchronizuotos 1 sekundės tikslumu iš dviejų sinchronizavimo šaltinių;
- Audituojamas visas tinklo duomenų srautas;
- Audituojamos duomenys archyvuojami ir centralizuotai saugomi.

Įsibrovimų aptikimas ir prevencija:

- Įdiegta automatizuota įsilaužimų aptikimo įranga;
- Įsilaužimo įvykiai klasifikuojami, audituojami ir nedelsiamai pranešama administratoriui;
- Įranga nuolat atnaujinama naudojant patikimus, aktualią informaciją teikiančius šaltinius;
- Įdiegtos ugniasienės, blokuojančios nenaudojamą įmonės veikloje įeinantį ir išeinantį duomenų srautą;
- Strateginė, įmonės veiklai svarbi KS įranga yra atjungta nuo bendro įmonės tinklo ir apjungta į atskirą vietinį tinklą.

Belaidžio tinklo saugumas ir kontrolė:

- Belaidžio tinklo įranga yra atskirta nuo vietinio tinklo;
- Belaidis tinklas yra valdomas ir prižiūrimas. Prisijungus neleistinam įrenginiui, pranešama administratoriui;
- Belaidžio ryšio duomenys yra šifruojami.

Svetainių, pasiekiamų iš viešųjų elektroninių ryšių tinklų, saugumas ir kontrolė:

- Svetainės atitinka tapatumo patvirtinimo reikalavimus;
- Duomenys yra šifruojami taikant patikimas šifravimo tarnybas;
- Svetainės atitinka kriptografijos reikalavimams;
- Taikomos SQL įsiskverbimo apsaugos.

3.3. Pažeidžiamumų ir grėsmių nustatymas

Pagal įmonės charakteristika ir analizę nustatomos galimos rizikos, kurios yra pateiktos 8 lentelėje. Nustatytoms rizikoms atrankos būdu yra priskiriamos aktualios grėsmės ir pažeidžiamumai. Pavyzdžiui, Laboratorijos duomenų suklastojimas negali būti susietas su radiacijos spinduliuotės poveikiu, todėl tai nėra pažeidžiamumas, bet personalo stebėjimo mechanizmų trūkumas – tai galimas pažeidžiamumas, dėl kurio gali įvykti neteisėtas duomenų apdorojimas, kuris gali sukelti laboratorijos duomenų suklastojimo riziką.

9 lentelė. Nustatytos rizikos, grėsmės ir pažeidžiamumai pagal ISO/IEC 27005

Nr.	Veiklos procesai / nustatytos rizikos	Pažeidžiamumų kiekis	Grėsmės
Gamybiniai procesai			
1.	Technologijos valdymo sutrikimas	20	12
2.	Technologijos stebėjimo sutrikimas	11	9
Laboratoriniai procesai			
3.	Laboratorijos veiklos sutrikimas	10	7
4.	Laboratorijos duomenų praradimas / suklastojimas	14	7
Paslaugų tiekimo procesai			
5.	Paslaugų tiekimo valdymo sutrikimas	12	7
6.	Paslaugų tiekimo stebėjimo sutrikimas	6	6
Klientų aptarnavimo procesai			
7.	Klientų aptarnavimo procesų sutrikimas	23	9
8.	Klientų duomenų nutekėjimas / praradimas	16	10
Vidaus resursų ir išteklių valdymo procesai			
9.	Finansų apskaitos valdymo procesų sutrikimas	17	10
10.	Finansų apskaitos duomenų praradimas	18	9
11.	Atsargų ir išteklių valdymo procesų sutrikimas	14	12
12.	Atsargų ir išteklių valdymo duomenų praradimas	18	9
13.	Personalo valdymo procesų sutrikimas	14	12
14.	Personalo duomenų praradimas	18	9
Ryšių su visuomene procesai			
15.	Ryšių su visuomene duomenų paviešinimas	12	11
16.	Ryšių su visuomene duomenų praradimas	7	5

Nustatyta, kad didžiausia pažeidžiamumų kiekį turi klientų aptarnavimo procesų rizika – 23 vnt. Antroje vietoje pagal pažeidžiamumų kiekį yra Technologijų valdymo sutrikimų rizika – 20 vnt. Trečią vietą užima finansų apskaitos duomenų praradimo, atsargų ir išteklių valdymo duomenų praradimo, personalo duomenų praradimo rizikos – 18 vnt. Mažiausia pažeidžiamumų kiekį turi paslaugų tiekimo stebėjimo rizika, kuri turi 6 pažeidžiamumus.

Atsižvelgiant į grėsmių kiekį nustatyta, kad daugiausia grėsmių turi technologijos, atsargų ir išteklių, personalo valdymo procesų sutrikimų rizikos, kurių grėsmių dydis sudaro – 12 vnt. Ryšių su visuomene duomenų paviešinimo rizikos grėsmių kiekis – 11 vnt. Klientų duomenų nutekėjimo / praradimo, finansų apskaitos valdymo sutrikimų rizikos turi – po 10 grėsmių.

3.4. Personalo apklausa

Įmonėje buvo apklausti IT specialistai, atsakingi už IT infrastruktūros funkcionavimą. Jiems buvo duota apklausos anketa, kuri pateikta šio darbo 6 priede. Ją sudarė 12 klausimų, sugrupuotų pagal įmonės vykdomus procesus, kurie formuoja rizikas. Apklausos rezultatų vertinimo metodika pateikta 7 priede.

1 – 4 klausimų rezultatai sumuojami. Didžiausias rezultatas – 4 balai. 1 balas atitinka 0,25 balo galimo nuostolių lygio ir grėsmės realizavimo tikimybės kriterijų lygiui.

5 – 6 klausimo rezultatai sumuojami. Didžiausias rezultatas – 4 balai. 1 balas atitinka 0,25 balo galimo nuostolių lygio ir grėsmės realizavimo tikimybės kriterijų lygiui.

7 – 8 klausimo rezultatai sumuojami. Didžiausias rezultatas – 4 balai. 1 balas atitinka 0,25 balo galimo nuostolių lygio ir grėsmės realizavimo tikimybės kriterijų lygiui.

9 klausimo didžiausias rezultatas – 4 balai. 1 balas atitinka 0,25 balo galimo nuostolių lygio ir grėsmės realizavimo tikimybės kriterijų lygiui.

10 – 11 klausimo rezultatai sumuojami. Didžiausias rezultatas – 4 balai. 1 balas atitinka 0,25 balo galimo nuostolių lygio ir grėsmės realizavimo tikimybės kriterijų lygiui.

12 klausimo didžiausias rezultatas – 4 balai. 1 balas atitinka 0,25 balo galimo nuostolių lygio ir grėsmės realizavimo tikimybės kriterijų lygiui.

Apklausos rezultatai yra pateikti 9 lentelėje. Apklausos metu yra nustatyti pažeidžiamumų išnaudojimo asmenų potencialas, taikomų prevencijos priemonių efektyvumas, informacinių sistemų kritiškumas, procesų pažeidžiamumų lygis, organizacijos veiklos reguliavimas ir reputacijos lygis.

10 lentelė. Personalo apklausos rezultatai

Nr.	Nustatytos rizikos	Apklausos rezultatai					
		IS kritiškumas	Procesų pažeidžiamumo lygis	Organizacijos veiklos reguliavimas	Reputacijos lygis	Grėsmės arba pažeidžiamumo išnaudojimo asmenų potencialas	Taikomų prevencijos priemonių efektyvumas
1.	Technologijos valdymo sutrikimas	1,5	3	2,5	1	3	2,5
2.	Technologijos stebėjimo sutrikimas	0,5	1	1	1	4	2,5
3.	Laboratorijos veiklos sutrikimas	2,5	4	3	3	3	2,5
4.	Laboratorijos duomenų praradimas / suklastojimas	1,5	2	2	1	3	1
5.	Paslaugų tiekimo valdymo sutrikimas	1,5	2	2	4	3	2,5
6.	Paslaugų tiekimo stebėjimo sutrikimas	1,5	1,5	1	1	3	3,5
7.	Klientų aptarnavimo procesų sutrikimas	3	4	3,5	3	3	0
8.	Klientų duomenų nutekėjimas / praradimas	0,5	2	3,5	3	4	0
9.	Finansų apskaitos valdymo procesų sutrikimas	2,8	4	3,5	3	3	0
10.	Finansų apskaitos duomenų praradimas	2,5	3	3,5	3	4	0
11.	Atsargų ir išteklų valdymo procesų sutrikimas	2,8	4	3,5	3	3	0
12.	Atsargų ir išteklų valdymo duomenų praradimas	2,5	2	2,5	1	4	0
13.	Personalo valdymo procesų sutrikimas	2	4	2	4	3	2,5
14.	Personalo duomenų praradimas	1,5	2	2,5	1	4	0
15.	Ryšių su visuomene duomenų paviešinimas	2,5	1	2,5	2	2,5	1,5
16.	Ryšių su visuomene duomenų praradimas	2,5	1,5	1	1	3	1,5

Pagal gautus apklausos duomenis nustatyta, kad didžiausia IS kritiškumą turi klientų aptarnavimo procesai – 3 balai, finansų apskaitos valdymo procesai, atsargų ir išteklų valdymo procesai – 2,75 balų. Trečioje vietoje – Laboratorijos veikla, finansų apskaitos bei atsargų ir išteklų duomenys, ryšių su visuomene duomenų paviešinimas – 2,5 balų.

Didžiausią pažeidžiamumo lygį turi daug procesų: laboratorijos veiklos sutrikimas, klientų aptarnavimo, finansų apskaitos valdymo, atsargų ir išteklų valdymo, personalo valdymo procesų sutrikimai, kurių dydis yra 4 balai.

Pagal veiklos reguliavimą didžiausius rezultatus turi klientų aptarnavimo procesų sutrikimas, klientų duomenų nutekėjimas / praradimas, finansų apskaitos duomenų praradimas, finansų apskaitos, atsargų ir išteklų valdymo procesų sutrikimai, kurių dydis – 3,5 balų.

Didžiausią įtaką organizacijos reputacijai turi: paslaugų tiekimo valdymo sutrikimai, personalo valdymo sutrikimai, kurių rezultatų dydis lygus 4 balams.

Technologijos stebėjimas, klientų, finansų apskaitos, atsargų ir išteklų, personalo valdymo duomenys, turi didžiausia išnaudojimo asmenų potencialą – 4 balai.

Pagal taikomųjų prevencijos priemonių efektyvumą, pirmauja 7 procesai. Mažiausią efektyvumą turi paslaugų stebėjimo procesas – 3,5 balo. 10 lentelėje rezultatai yra perskaičiuojami pagal 7 priede pateiktą metodiką tolimesniam rizikos vertinimui.

11 lentelė. Personalo apklausos rezultatų perskaičiuoti rezultatai

Nr.	Nustatytos rizikos	Apklausos rezultatai					
		IS kritiškumas	Procesų pažeidžiamumo lygis	Organizacijos veiklos reguliavimas	Reputacijos lygis	Grėsmės arba pažeidžiamumo išnaudojimo asmenų potencialas	Taikomų prevencijos priemonių efektyvumas
1.	Technologijos valdymo sutrikimas	0,5	0,75	0,75	0,25	0,75	0,75
2.	Technologijos stebėjimo sutrikimas	0,3	0,25	0,25	0,25	1	0,75
3.	Laboratorijos veiklos sutrikimas	0,8	1	0,75	0,75	0,75	0,75
4.	Laboratorijos duomenų praradimas / suklastojimas	0,5	0,5	0,5	0,25	0,75	0,25
5.	Paslaugų tiekimo valdymo sutrikimas	0,5	0,5	0,5	1	0,75	0,75
6.	Paslaugų tiekimo stebėjimo sutrikimas	0,5	0,5	0,25	0,25	0,75	1
7.	Klientų aptarnavimo procesų sutrikimas	0,8	1	1	0,75	0,75	0
8.	Klientų duomenų nutekėjimas / praradimas	0,3	0,5	1	0,75	1	0
9.	Finansų apskaitos valdymo procesų sutrikimas	0,8	1	1	0,75	0,75	0
10.	Finansų apskaitos duomenų praradimas	0,8	0,75	1	0,75	1	0
11.	Atsargų ir išteklių valdymo procesų sutrikimas	0,8	1	1	0,75	0,75	0
12.	Atsargų ir išteklių valdymo duomenų praradimas	0,8	0,5	0,75	0,25	1	0
13.	Personalo valdymo procesų sutrikimas	0,5	1	0,5	1	0,75	0,75
14.	Personalo duomenų praradimas	0,5	0,5	0,75	0,25	1	0
15.	Ryšių su visuomene duomenų paviešinimas	0,8	0,25	0,75	0,5	0,75	0,5
16.	Ryšių su visuomene duomenų praradimas	0,8	0,5	0,25	0,25	0,75	0,5

3.5. Galimo žalos lygio, grėsmių realizavimo tikimybės ir rizikų įvertinimas

Pagal 1 žingsnyje pateiktą organizacijos charakteristiką nustatomi duomenų kategorijos koeficientai. 11 lentelėje pateikti grėsmių realizavimo tikimybės P(t) skaičiavimai.

12 lentelė. Grėsmės realizavimo tikimybės skaičiavimai

Nr.	Nustatytos rizikos	Aktyvių grėsmių kiekis	Aktyvių pažeidžiamumų kiekis	Grėsmės arba pažeidžiamumo išnaudojimo asmenų potencialas	Taikomų prevencijos	P(t)
1.	Technologijos valdymo sutrikimas	1,00	0,87	0,75	0,75	3,37
2.	Technologijos stebėjimo sutrikimas	0,75	0,48	1	0,75	2,98
3.	Laboratorijos veiklos sutrikimas	0,58	0,43	0,75	0,75	2,52
4.	Laboratorijos duomenų praradimas / suklastojimas	0,58	0,61	0,75	0,25	2,19
5.	Paslaugų tiekimo valdymo sutrikimas	0,58	0,52	0,75	0,75	2,61
6.	Paslaugų tiekimo stebėjimo sutrikimas	0,50	0,26	0,75	1	2,51
7.	Klientų aptarnavimo procesų sutrikimas	0,75	0,00	0,75	0	1,50
8.	Klientų duomenų nutekėjimas / praradimas	0,83	0,70	1	0	2,53
9.	Finansų apskaitos valdymo procesų sutrikimas	0,83	0,74	0,75	0	2,32
10.	Finansų apskaitos duomenų praradimas	0,75	0,78	1	0	2,53
11.	Atsargų ir išteklių valdymo procesų sutrikimas	1,00	0,61	0,75	0	2,36
12.	Atsargų ir išteklių valdymo duomenų praradimas	0,75	0,78	1	0	2,53
13.	Personalo valdymo procesų sutrikimas	1,00	0,61	0,75	0,75	3,11
14.	Personalo duomenų praradimas	0,75	0,78	1	0	2,53
15.	Ryšių su visuomene duomenų paviešinimas	0,92	0,52	0,75	0,5	2,69
16.	Ryšių su visuomene duomenų praradimas	0,42	0,30	0,75	0,5	1,97

Šiuo atveju yra perskaičiuotos grėsmių ir pažeidžiamumų reikšmės, pagal 7 paveiksle pateiktą pavyzdį, kuomet $T_{max} = 12$; $A_{max} = 23$. Gauti rezultatai rodo, kad didžiausia grėsmės realizavimo

tikimybę sudaro technologijos valdymo procesai – 3,37 balo. Antroje vietoje personalo valdymo procesai – 3,11 balo. Trečią vietą užima technologijos stebėjimo sutrikimai – 2,98 balo. 12 lentelėje pateikti galimo žalos lygio skaičiavimai. Mažiausia grėsmės realizavimo tikimybę sudaro klientų aptarnavimo procesų sutrikimas – 1,5 balo.

13 lentelė. Galimo žalos lygio skaičiavimai

Nr.	Nustatytos rizikos	Duomenų kategorija	IS kritiškumas	Procesų pažeidžiamumo lygis	Organizacijos veiklos	Reputacijos lygis	S
1.	Technologijos valdymo sutrikimas	0,75	0,5	0,75	0,75	0,25	3,00
2.	Technologijos stebėjimo sutrikimas	0,75	0,25	0,25	0,25	0,25	1,75
3.	Laboratorijos veiklos sutrikimas	0,75	0,75	1	0,75	0,75	4,00
4.	Laboratorijos duomenų praradimas / suklastojimas	0,75	0,5	0,5	0,5	0,25	2,50
5.	Paslaugų tiekimo valdymo sutrikimas	0,75	0,5	0,5	0,5	1	3,25
6.	Paslaugų tiekimo stebėjimo sutrikimas	0,75	0,5	0,5	0,25	0,25	2,25
7.	Klientų aptarnavimo procesų sutrikimas	1,00	0,75	1	1	0,75	4,50
8.	Klientų duomenų nutekėjimas / praradimas	1,00	0,25	0,5	1	0,75	3,50
9.	Finansų apskaitos valdymo procesų sutrikimas	0,50	0,75	1	1	0,75	4,00
10.	Finansų apskaitos duomenų praradimas	0,50	0,75	0,75	1	0,75	3,75
11.	Atsargų ir išteklių valdymo procesų sutrikimas	0,50	0,75	1	1	0,75	4,00
12.	Atsargų ir išteklių valdymo duomenų praradimas	0,50	0,75	0,5	0,75	0,25	2,75
13.	Personalo valdymo procesų sutrikimas	0,50	0,5	1	0,5	1	3,50
14.	Personalo duomenų praradimas	0,50	0,5	0,5	0,75	0,25	2,50
15.	Ryšių su visuomene duomenų paviešinimas	0,25	0,75	0,25	0,75	0,5	2,50
16.	Ryšių su visuomene duomenų praradimas	0,25	0,75	0,5	0,25	0,25	2,00

Nustatyta, kad didžiausią žalą sudaro klientų aptarnavimo procesų sutrikimai – 4,5 balo, laboratorijos veiklos, finansų apskaitos bei atsargų ir išteklių valdymo procesų sutrikimai 4 balai, finansų apskaitos duomenų praradimas – 3,75 balo. Mažiausią žalą sudaro technologijos stebėjimo sutrikimai – 1,75 balo. Pagal NIST 800-30 formulę $R = P(t) * S$ vertinamos rizikos. Rizikų vertinimo rezultatai pateikti 13 lentelėje.

14 lentelė. Rizikos vertinimo rezultatai

Nr.	Nustatytos rizikos	P(t)	S	R
1.	Technologijos valdymo sutrikimas	3,37	3,00	10
2.	Technologijos stebėjimo sutrikimas	2,98	1,75	5
3.	Laboratorijos veiklos sutrikimas	2,52	4,00	10
4.	Laboratorijos duomenų praradimas / suklastojimas	2,19	2,50	5
5.	Paslaugų tiekimo valdymo sutrikimas	2,61	3,25	8
6.	Paslaugų tiekimo stebėjimo sutrikimas	2,51	2,25	6
7.	Klientų aptarnavimo procesų sutrikimas	1,50	4,50	7
8.	Klientų duomenų nutekėjimas / praradimas	2,53	3,50	9
9.	Finansų apskaitos valdymo procesų sutrikimas	2,32	4,00	9
10.	Finansų apskaitos duomenų praradimas	2,53	3,75	9
11.	Atsargų ir išteklių valdymo procesų sutrikimas	2,36	4,00	9
12.	Atsargų ir išteklių valdymo duomenų praradimas	2,53	2,75	7
13.	Personalo valdymo procesų sutrikimas	3,11	3,50	11
14.	Personalo duomenų praradimas	2,53	2,50	6
15.	Ryšių su visuomene duomenų paviešinimas	2,69	2,50	7
16.	Ryšių su visuomene duomenų praradimas	1,97	2,00	4

Nustatyta, kad didžiausią riziką turi personalo valdymo procesų sutrikimas – 11 balų, technologijos valdymo ir laboratorijos veiklos sutrikimai – 10 balų. Finansų apskaitos bei atsargų ir išteklių valdymo procesų sutrikimų ir duomenų praradimo rizika lygi – 9 balams. Mažiausią riziką turi ryšių su visuomene duomenų praradimas – 4 balai. Laboratorijos duomenų praradimo / suklaidojimo ir technologijos sutrikimo rizika – 5 balai.

3.6. Rizikos rezultatų reitingavimas ir segmentavimas

Rizikos vertinimo rezultatai paverčiami procentinę išraišką ir segmentuojami į keturias grupes. Rizikos segmentavimo rezultatai pateikti 14 lentelėje.

15 lentelė. Rizikų segmentavimas

Nr.	Nustatytos rizikos	R	R (%)	R (segmentuota)
1.	Technologijos valdymo sutrikimas	10	51	Vidutinė
2.	Technologijos stebėjimo sutrikimas	5	26	Žema
3.	Laboratorijos veiklos sutrikimas	10	50	Vidutinė
4.	Laboratorijos duomenų praradimas / suklaidojimas	5	27	Vidutinė
5.	Paslaugų tiekimo valdymo sutrikimas	8	42	Vidutinė
6.	Paslaugų tiekimo stebėjimo sutrikimas	6	28	Vidutinė
7.	Klientų aptarnavimo procesų sutrikimas	7	34	Vidutinė
8.	Klientų duomenų nutekėjimas / praradimas	9	44	Vidutinė
9.	Finansų apskaitos valdymo procesų sutrikimas	9	46	Vidutinė
10.	Finansų apskaitos duomenų praradimas	9	47	Vidutinė
11.	Atsargų ir išteklių valdymo procesų sutrikimas	9	47	Vidutinė
12.	Atsargų ir išteklių valdymo duomenų praradimas	7	35	Vidutinė
13.	Personalo valdymo procesų sutrikimas	11	54	Aukšta
14.	Personalo duomenų praradimas	6	32	Vidutinė
15.	Ryšių su visuomene duomenų paviešinimas	7	34	Vidutinė
16.	Ryšių su visuomene duomenų praradimas	4	20	Žema

Pagal rizikos segmentavimo rezultatus nustatyta, kad personalo valdymo procesų sutrikimas turi aukštą rizikos lygį. Technologijos stebėjimo sutrikimo ir ryšių su visuomene duomenų praradimo rizikos turi žemą rizikos lygį. Kitos rizikos yra vidutinio lygio.

3.7. Rizikos mažinimas

Rizikos mažinimui parinkta rizika turinti didžiausią reikšmę – Personalo valdymo procesų sutrikimai

Proceso aprašymas - Personalo valdymas vykdomas buhalterinės apskaitos programinės įrangos pagalba. Sistema veikia kartu su finansinės apskaitos ir atsargų bei išteklių valdymo programine įranga, viename serveryje. Vartotojų teisės yra tinkamai paskirstytos, bet reikšmių pokytis bet kurioje išvardintų programų įtakoja kitus vidaus išteklių valdymo procesus. Duomenų bazė archyvuojama saugoma serveryje. Darbuotojai dirba taikant vardinę licenciją savo darbo vietoje, jungiantis prie serverio naudojant klientinę PĮ. 15 lentelėje pateikta atsakomųjų priemonių nustatymo forma, kurioje pateikti personalo valdymo proceso nustatyti pažeidžiamumai, kuriems yra parinktos atsakomosios

priemonės. Pritaikius atsakomąsias priemones pažeidžiamumams, jis tampa neaktyvus, taip prognozuojamas teigiamas rizikos pokytis.

16 lentelė. Atsakomųjų priemonių nustatymo forma

Nr.	Pažeidžiamumas	Pažeidžiamumo šaltinis	Atsakomosios priemonės
1.	Jautrumas įtampos šuoliams	Viena 10kV oro elektros tiekimo linija	-
2.	Neapsaugotas saugojimas	DB kopijos nėra šifruojamos ir atvira saugomi virtualiame serveryje	Archyvavimo metu apsaugoti slaptažodžiu
3.	Nepakankamas programinis testavimas, arba jo trūkumas	Atlikus PĮ atnaujinimą neveikia dalis funkcionalumo	Reikalauti PĮ tiekėjų atlikti papildomas PĮ patikras
4.	Sudėtinga vartotojų aplinka	Programinė įranga turi seną interfeisą, kuris buvo tobulinamas.	-
5.	Nustatytas neteisingas parametras	Po atnaujinimų keičiasi parametrai	Nustatyti nusimtus parametrus iš naujo, po kiekvieno PĮ atnaujinimo
6.	Turinti trūkumų arba nauja programinė įranga	Naujas funkcionalumas ne visada veikia korektiškai	Papildomai tikrinti naują PĮ funkcionalumą
7.	Efektyvios konfigūracijos pokyčių kontrolės trūkumai	Sunku atsekti atsiradusius trūkumus po PĮ funkcionalumo pakeitimo. Dažniausia išaiškėja kai to funkcionalumo reikia	Reikalauti darbuotojų reguliariai tikrinti reikalingą funkcionalumą po kiekvieno atnaujinimo
8.	Nevaldomas paleidimas ir programinės įrangos naudojimas	Darbuotojos gali netyčia paleisti tą pačią ataskaitą kelis kartus iš eilės, kas sukelia PĮ sutrikimus	Numatyti PĮ vienodo proceso paleidimo apsaugos priemones
9.	Netinkamas programinės ir kompiuterinės įrangos naudojimas	Darbuotojos laisvalaikio metu naršo internete, tvarko asmeninius dokumentus	Naršymo greičio ribojimas, srauto kontrolė in pastabų teikimas
10.	Saugumo supratimo trūkumai	Darbuotojai ginčijasi dėl saugumo reikalavimų ir nevykdo saugos tvarkos įsakymų	IT saugos seminarų organizavimas
11.	Netinkamas aptarnaujančio personalo atsakymas	Paaškinant PĮ klaidos esmę, darbuotojai klysta teikiant kompetingą informaciją IT personalui	Prašymas teikti informaciją raštu
12.	Tęstinumo planų trūkumai	IT dokumentacijoje nenumatyta pakankamai personalo valdymo proceso sutrikimų tęstinumo veiksmų	Peržiūrėti ir papildyti testinimo planus
13.	Įdiegtų valdymo mechanizmų, saugos taisyklių pažeidimo atveju trūkumas	Pažeidžiant saugos taisykles, ne visais atvejais įgyvendinamos sankcijos	Įdiegti papildomą PĮ atliekančią saugos auditą personaliniuose kompiuteriuose
14.	Pranešimo apie esamus saugos pažeidžiamumus proceso trūkumas	Kai darbuotojos padaro klaidą, arba pažeidžia saugumo reikalavimus (pavyzdžiui gautas fishingo laiškas), nepraneša apie tai IT personalui	Reikalauti nedelsiant pranešti apie IT saugumo pažeidimus

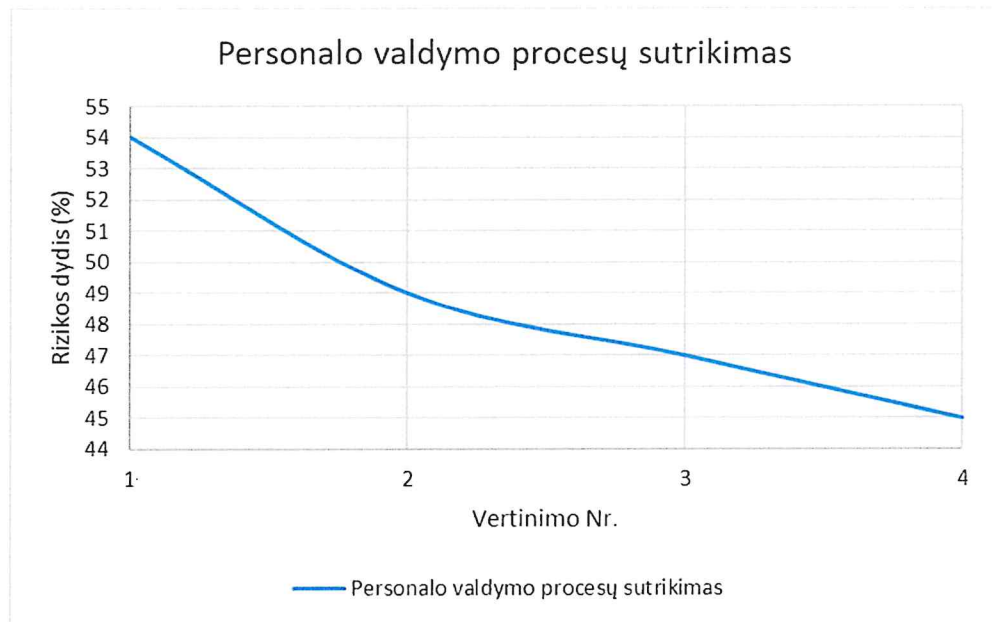
Pagal suteiktą nustatytų atsakomųjų priemonių formą, antram matavimui yra skiriamas dėmesys pažeidžiamumams Nr.: 2; 5; 9; 10; 12, kuriems yra pritaikomos atsakomosios priemonės:

- Neapsaugotas saugojimas (Nr. 2) – atsarginės kopijos archyvavimo metu, kopija apsaugoma slaptažodžiu ir perkeliama į D2D atsarginių kopijų saugojimo serverį, prie kurio turi prieigą tik IT personalas.
- Nustatytas neteisingas parametras (Nr. 5) – po kiekvieno PĮ atnaujinimo yra patikrinami baziniai PĮ parametrai, dėl kurių gali neveikti PĮ funkcionalumas.
- Netinkamas programinės ir kompiuterinės įrangos naudojimas (Nr. 9) – Kontroliuojamas tinklo srautas. Esant poreikiui kuriamos duomenų srauto greiti apribojančios taisyklės.

- Saugumo supratimo trūkumai (Nr. 10) – IT saugos seminarų organizavimas, siekiant pagerinti darbuotojų kompiuterinio raštingumo ir kibernetinio saugumo kompetencijas.
- Tęstinumo planų trūkumai (Nr. 12) – peržiurimą IT dokumentacija ir papildomas tęstinumo planas.

3.8. Rizikos jautrumo analizė

Pritaikius išvardintas atsakomąsias priemones pažeidžiamumų kiekis sumažėjo nuo 14 iki 9, grėsmių kiekis sumažėjo nuo 12 iki 11. Šiuo atveju „P(t)“ rodiklis lygus 2,81, „S“ rodiklis nekinta. Rizikos lygis sumažėjo nuo 11(54%) iki 10 balų (49%), dinamikos grafikas pateiktas 7 paveiksle. Rizikos skirtumą sudaro – 5%, ji segmentuojama iki „Vidutinės“ rizikos.



9 pav. Rizikos dinamika

P Nustatyta, kad pašalinus pažeidžiamumą Nr. 1, pažeidžiamumų kiekis sumažėjo nuo 9 iki 8, grėsmių kiekis sumažėjo nuo 11 iki 10, šiuo atveju „P(t)“ rodiklis lygus 2,68, „S“ rodiklis nekinta, rizikos rodiklis sumažėja nuo 10 balų (49%) iki 9 (47%), skirtumą sudaro 2%.

Pašalinus pažeidžiamumą Nr. 3, pažeidžiamumų kiekis sumažėjo nuo 8 iki 7, grėsmių kiekis sumažėjo nuo 10 iki 9, šiuo atveju „P(t)“ rodiklis lygus 2,55, „S“ rodiklis nekinta, rizikos rodiklis sumažėja nuo 10 balų (47%) iki 9 (45%), skirtumą sudaro 2%.

Rizikos yra nejautrios galimos žalos lygio (S) atžvilgiu. Jautrios grėsmės realizavimo tikimybės atžvilgiu (P(t)). Rizikos jautrumas priklauso nuo pažeidžiamumo kuris išnaudojamas tam tikru grėsmių kiekiu.

4. Metodo patobulinimo rezultatų analizė ir rekomendacijos

Praktinio pritaikymo metu nustatyta, kad 13 rizikų lygis yra „vidutinis“, 2 rizikų – „žemas“, 1 rizika yra „aukšto“ lygio. Segmentuojant sprendimus, yra patogu vizualizuoti gautus rezultatus. Matematinio modelio analitinio metodo taikymas padeda įvertinti organizacijoje esamas rizikas.

Rizikos rezultatai priklauso nuo dviejų rizikos rodiklių – grėsmės realizavimo tikimybės ir galimos žalos lygio. Grėsmės realizavimo tikimybės reikšmė priklauso nuo aktyvių pažeidžiamumų ir grėsmių kiekio. 7 paveiksle pateiktas grafikas rodo, kad ,keičiantis pažeidžiamumų kiekiui, rizika kinta netolygiai, pagal neapibrėžtą funkciją. Pagal rizikos jautrumo analizės rezultatus nustatyta, kad, kintant pažeidžiamumų kiekiui, grėsmių kiekis kinta neproporcingai. Grėsmių pokytis priklauso nuo pažeidžiamumo pobūdžio. Viena grėsmė gali išnaudoti kelis skirtingus pažeidžiamumus. Tai rodo 8 lentelės rezultatai, kai rizikos Nr. 7 didžiausias pažeidžiamumų kiekis (23 vnt.) turi tik 9 grėsmes. Tuomet pagal 13 lentelės rezultatus nustatytas rizikos lygio rezultatas yra 7 iš 20 balų.

Grėsmės išnaudotojo potencialo ir taikomų priemonių efektyvumo rodikliai yra pastovūs ir nekinta rizikos mažinimo etapo metu. Galimos žalos lygis nustatomas pagal gautus organizacijos charakteristikos ir personalo apklausos duomenis. Šis rizikos rodiklis taip pat yra pastovus ir nekinta rizikos mažinimo etapo metu. Tai įrodo 13 lentelėje pateikti duomenys.

Patobulinto rizikos valdymo metodas leidžia greitai ir akivaizdžiai įvertinti IT infrastruktūros rizikas organizacijoje. Rezultatai įrodo patobulinto metodo privalumą ir trūkumus.

4.1. Patobulinto metodo privalumas

Patobulintame metode išvengiama turto įvertinimo galimybė. Visas dėmesys skirtas techninėms IT rizikoms. Metodas veikia neturint statistinių duomenų dėl įvykusių kibernetinių incidentų ir veikia visiško neapibrėžtumo pagrindu. Organizacijos auditavimo procesai (1–4 žingsniai) padeda surinkti tinkamą informaciją apie organizacijos IT infrastruktūros būklę ir nustatyti objektyvias rizikas. Pažeidžiamumų ir grėsmių nustatymo procesas vykdomas vadovaujantis ISO/IEC 27005 standartu. Rizikos vertinimas vyksta grėsmės realizavimo tikimybės ir galimo žalos lygio santykio pagrindu. Toks sprendimas leidžia greitai ir lengvai nustatyti rizikos rodiklius ir įvertinti jų koeficientus pagal pateiktą metodologiją. Rizikos vertinimo procesas yra patogus, paprastas, aiškus ir nereikalauja vykdytojo specifinių žinių arba kompetencijų. Rizikos jautrumo analizės pagrindu lengva įvertinti pažeidžiamumų bei grėsmių įtaką rizikai, esant tam tikroms sąlygoms, ir nustatyti rizikos rodiklių pokyčio priklausomybę nuo pažeidžiamumų pokyčio. Rizikos vertinimo rezultatai yra išreiškiami balais ir aiškiai vizualizuojami taikant rezultatų segmentavimo sprendimus.

4.2. Patobulinto metodo trūkumai

81,25 % rizikų buvo segmentuotos kaip „vidutinės“. Tai rodo, kad vidutinis rizikos balas svyruoja nuo 6 iki 10. Pagal pasirinktą segmentavimo į 4 kategorijas būdą neįmanoma tiksliai nustatyti rizikos prioritetų vienoje kategorijoje. Kadangi rizikos rezultatai, esant pažeidžiamųjų pokyčiui, kinta neproporcingai, teigiama, kad kiekviena rizika kinta pagal neapibrėžtą funkciją. Tokiu atveju rizikos rezultatų proporcingas segmentavimas, kurio pavyzdys pateiktas 4 paveiksle, netiksliai įvertina rizikos rezultatus.

4.3. Rekomendacijos

Sukurtame metode siūloma atsižvelgti į rezultatų segmentavimo sprendimus. Tam, kad rezultatų segmentavimas perteiktų objektyvius duomenis, reikia įvertinti kiekvienos rizikos priklausomybes nuo nustatytų pažeidžiamųjų ir papildyti valdymo metodo procedūrą papildomos analizės procesu. Kiekviena nustatyta rizika bus analizuojama dėl kiekvieno pažeidžiamumo įtakos, ir kiekvienas rezultatas bus segmentuojamas pagal atskirai nustatytą priklausomybės funkciją. Tokiu atveju rizikos jautrumo analizės žingsnis bus nereikalingas, o 20 balų rezultatų reitingavimo riba bus netinkama rizikos segmentavimui. Tuomet siūloma nustatyti ribas, atsižvelgiant į gautus rizikos rezultatus balais. Kiekvieno rizikos vertinimo proceso metu bus gaunamas skirtingas maksimalus rezultatas, kuris bus lygus aukštam rizikos lygiui.

Metodas turi daug tobulinimo galimybių. Tai:

- vartotojo programos kūrimas, kurioje bus suvedami reikalingi duomenys ir rizikos vertinimo procesas bus vykdomas automatiškai būdu, nustatytus atitinkamus pažeidžiamumus;
- galimybė naudoti OWASP bibliotekas arba lygiavertes duomenų bazes pažeidžiamųjų ir grėsmių nustatymui;
- dirbtinio intelekto taikymas nustatant rizikos rodiklius;
- ekspertinės sistemos kūrimas, kuri, remdamasi gautais rizikos rezultatais, teiktų rizikos mažinimo rekomendacijas.

Išvados

Iš atliktos kibernetinės saugos situacijos apžvalgos matyti, kad kibernetinės saugos klausimas šiuolaikiniame pasaulyje yra itin svarbus. Kibernetinėje erdvėje aktyviai veikia įvairios kibernetinių nusikaltėlių grupės ir tarptautiniai teroristai, šnipinėdami ekonominėje, civilinėje ir karinėje srityse, jie bando sustabdyti įmonių, įstaigų, organizacijų ir kitų IT infrastruktūrą turinčių objektų veiklą. Lietuvoje saugos sistema ir jos taikymas nepakankamai efektyvus, poreikiai ir rizikos yra vertinamos netinkamai.

Pažeidžiamumų nustatymas parodė, kad pažeidžiamumas pats nekenkia, turi būti grėsmė, leidžianti išnaudoti šį pažeidžiamumą. Grėsmės nesukelia rizikos be pažeidžiamumų išnaudojimo, tačiau jas reikia rasti ir stebėti pokyčius. Grėsmės įvairiuose literatūros šaltiniuose apibrėžiamos skirtingai.

IT rizikos valdymo metodų analizės metu nustatyta, kad IT rizika, arba kibernetinė rizika, yra tiesiogiai susijusi su informacinėmis technologijomis. Informacija vertinama kaip vertingas ir svarbus turtas, žinių, ekonomikos augimas ir skaitmeninė revoliucija paskatino organizacijas vis labiau priklausyti nuo informacijos, jos apdorojimo ir informacinių technologijų priemonių. Yra daug metodikų, kurios atitinka kibernetinės saugos rizikos valdymo poreikius. Kiekviena turi savo privalumų ir trūkumų. Rizikos valdymo methoduose nėra aiškiai reglamentuojamas techninių rizikų valdymas.

Naudojant patobulintą metodą nustatyta, kad tiriamos organizacijos personalo valdymo procesų sutrikimų rizikos lygis – aukštas. Taikant pasiūlytas priemones rizika sumažinta iki vidutinio lygio. Rizikų, pažeidžiamumų ir grėsmių nustatymo bei įvertinimo žingsniai leido tiksliai nustatyti IT infrastruktūros rizikas organizacijoje. Iš patobulinto ir pritaikyto metodo jautrumo analizės rezultatų matyti rizikos rezultatų priklausomybė nuo dviejų rizikos rodiklių: grėsmės realizavimo tikimybės – $P(t)$ ir galimos žalos lygio – S . Kadangi rizikos rezultatai, esant pažeidžiamumų pokyčiui, kinta neproporcingai, rizikos rezultatų segmentavimas duoda netikslius rezultatus. Tai yra pagrindinis patobulinto metodo trūkumas. Sukurtame metode siūloma atsižvelgti į rezultatų segmentavimo sprendimų papildomą patobulinimą.

Literatūros sąrašas

1. Europos Sąjungos Pagrindinių teisių chartija [interaktyvus]. Briuselis, 2012 [žiūrėta 2019 m. vasario 3 d.]. Prieiga per internetą:
<http://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A12012P%2FTXT>
2. Europos Parlamento ir Tarybos direktyvos 95/46/EB - dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo nuostatos [interaktyvus]. Briuselis, 1995. Briuselis, 2012 [žiūrėta 2019 m. vasario 3 d.]. Prieiga per internetą:
<http://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:31995L0046&from=LT>
3. BDAR - Asmens duomenų apsaugos reforma [interaktyvus]. Briuselis, 2016. [žiūrėta 2019 m. vasario 4 d.]. Prieiga per internetą: <https://www.consilium.europa.eu/lt/policies/data-protection-reform/>
4. Europos komisijos pranešimas spaudai. Komisija siūlo visapusišką duomenų apsaugos taisyklių reformą, kad vartotojai labiau kontroliuotų savo duomenis ir sumažėtų įmonių sąnaudos [interaktyvus]. 2012. [žiūrėta 2019 m. vasario 5 d.]. Prieiga per internetą:
http://europa.eu/rapid/press-release_IP-12-46_lt.htm
5. Europos Parlamento ir Tarybos direktyva ES – Dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR [interaktyvus]. Briuselis, 2008. [žiūrėta 2019 m. vasario 5 d.]. Prieiga per internetą:
<https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016L0680R%2801%29>
6. Irwin Barry V.W. 2013. Standing your ground: current and future challenges in cyber defense / Theories and Intricacies of Information Security Problems. Potsdam: Universitätsverlag. 100 – 108.
7. Stulz, M. 2008. Risk Management Failures: What Are They and When Do They Happen? *Journal of Applied Corporate Finance*: 58-67.
8. Пашковская М.В., Господарик Ю.П. 2016. Международная экономика безопасности. Москва: Университет «Синергия».
9. Sejník V. 2008. Struggle Against Cybercrime as Part of International Security [interaktyvus]. Computer Crime Research Center, 2008. [žiūrėta 2019 m. vasario 6 d.]. Prieiga per internetą:
<http://www.crimeresearch.ru/articles/Sejnik/>
10. Passeri P. 2019. Hackmageddon – Information Security Timelines and Statistics. [žiūrėta 2019 m. vasario 7 d.]. Prieiga per internetą: <https://www.hackmageddon.com/2019/02/04/15-january-2019-cyber-attacks-timeline/>

11. The Three Biggest Cyber-Attacks of 2016 [interaktyvus]. [žiūrėta 2019 m. vasario 7 d.]. Prieiga per internetą: <http://www.rheagroup.com/three-biggest-cyber-attacks-2016/>
12. Global Cybersecurity Index and Cyberwellness Profiles Report. 2015. Geneva: ABI Research. 13-14
13. ENISA – organizacijos aprašymas [interaktyvus]. Briuselis, 2012. [žiūrėta 2019 m. vasario 8 d.]. Prieiga per internetą: <https://www.enisa.europa.eu/about-enisa>
14. First EU Cyber Security Exercise Cyber Europe 2010 with 320 incidents successfully concluded [interaktyvus]. Briuselis, 2010. [žiūrėta 2019 m. vasario 8 d.]. Prieiga per internetą: <https://www.enisa.europa.eu/news/enisa-news/cyber-europe-20102019-cyber-security-exercise-with-320-2018incidents2019-successfully-concluded>
15. Nizhegorodcev D. 2014. European cybercrime centre sums up its first year work [interaktyvus]. [žiūrėta 2019 m. vasario 9 d.]. Prieiga per internetą: <https://vz.ru/news/2014/2/11/671970.html>
16. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [interaktyvus]. Briuselis, 2013. [žiūrėta 2019 m. vasario 10 d.]. Prieiga per internetą: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
17. Haeni R. 2016. Cybersecurity: New EU Directive Published. 2016. [interaktyvus]. [žiūrėta 2019 m. vasario 12 d.]. Prieiga per internetą: <https://news.pwc.ch/28616/cybersecurity-new-eu-directive-published>
18. Schreier F.; Weekes B.; Winkler T.H. 2015. Cybersecurity: The Road Ahead [interaktyvus]. Geneva: Centre for the Democratic Control of Armed Forces, Horizon. [žiūrėta 2019 m. vasario 14 d.]. Prieiga per internetą: <https://dcaf.ch/sites/default/files/publications/documents/Cyber2.pdf>
19. GDPR - General Data Protection Regulation [interaktyvus]. Briuselis, 2016. [žiūrėta 2019 m. vasario 15 d.]. Prieiga per internetą: <https://gdpr-info.eu/>
20. Kibernetinio saugumo įstatymas [interaktyvus]. Vilnius, 2014. [žiūrėta 2019 m. vasario 16 d.]. Prieiga per internetą: <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee>
21. Valstybės informacinių išteklių valdymo įstatymas [interaktyvus]. Vilnius, 2011. [žiūrėta 2019 m. sausio 25 d.]. Prieiga per internetą: <https://www.e-tar.lt/portal/lt/legalAct/TAR.85C510BA700A>

22. ES bendradarbiavimo saugumo ir gynybos srityje chronologija [interaktyvus]. Briuselis, 2018. [žiūrėta 2019 m. vasario 17 d.]. Prieiga per internetą: <https://www.consilium.europa.eu/lt/policies/defence-security/defence-security-timeline/>
23. Nacionalinis kibernetinio saugumo centras prie krašto apsaugos ministerijos – Nacionalinio kibernetinio saugumo būklės ataskaita [interaktyvus]. Vilnius, 2017. [žiūrėta 2019 m. vasario 18 d.]. Prieiga per internetą: https://kam.lt/download/61258/nksc%20ataskaita_final.pdf
24. Nacionalinis kibernetinės saugos indeksas [interaktyvus]. Estija, 2019. [žiūrėta 2019 m. vasario 19 d.]. Prieiga per internetą: <https://ncsi.ega.ee/ncsi-index/>
25. Kibernetinio saugumo apžvalga (2016) ISSN 1392-6721. Vilnius: UAB „Petro ofsetas“. 3-4.
26. IT audito gairės [interaktyvus]. Vilnius, 2018. [žiūrėta 2019 m. kovo 17 d.]. Prieiga per internetą: https://www.vkontrole.lt/INTOSAI_standartai/TAAIS_5300_2016_LT.pdf
27. Shirey R. Internet Engineering Task Force RFC 2828 Internet Security Glossary [interaktyvus]. GTE / BBN Technologies, 2000. [žiūrėta 2019 m. kovo 30 d.]. Prieiga per internetą: <https://www.ietf.org/rfc/rfc2828.txt>
28. ISO/IEC ISO/IEC 27005:2018 – Information technology – Security techniques – Information security risk management [interaktyvus]. Briuselis, 2018. [žiūrėta 2019 m. balandžio 3 d.]. Prieiga per internetą: https://view.elaba.lt/standartai/view?search_from=aleph&id=1273235
29. Stulz, M. 2008. Risk Management Failures: What Are They and When Do They Happen? Journal of Applied Corporate Finance: 58-67.
30. Vidaus reikalų ministerija, Rizikos analizės vadovas [interaktyvus]. Vilnius, 2005. 45-46. [žiūrėta 2019 m. balandžio 11 d.]. Prieiga per internetą: https://www.nksc.lt/doc/rizikos_analize.pdf
31. Октаева Е. В. 2016. Математические модели и методы оценки рисков. Казань: Молодой ученый. 310 – 313.
32. Уродовских В. Н. 2009. Управление рисками предприятия: Учеб. пособие. Москва: ВЗФЭИ. 130.
33. Слабинский С. В. 2014. Особенности оценки рисков в производственной деятельности промышленных предприятий ISSN: 1810-4894. Воронеж: Воронежский государственный технический университет.
34. CNSS Instruction No. 4009 [interaktyvus]. Committee on National Security Systems, 2015. [žiūrėta 2019 m. balandžio 11 d.]. Prieiga per internetą: <https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf>
35. National Information Assurance Certification and Accreditation Process (NIACAP) [interaktyvus] Committee on National Security Systems, 2015. [žiūrėta 2019 m. balandžio 11 d.]. Prieiga per internetą:

- <https://web.archive.org/web/20080807172156/http://www.cnss.gov/Assets/pdf/CNSSP-6.PDF>
36. NIST SP 800-30 – Risk Management Guide for Information Technology Systems [interaktyvus]. Gatesburg, 2012. [žiūrėta 2019 m. balandžio 11 d.]. Prieiga per internetą: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
 37. FIPS Publication 200 Minimum Security Requirements for Federal Information and Information Systems [interaktyvus]. Gatesburg, 2014. [žiūrėta 2019 m. balandžio 15 d.]. Prieiga per internetą: <https://csrc.nist.gov/publications/detail/fips/200/final>
 38. ISACA The Risk IT Framework ISBN 978-1-60420-111-6 [interaktyvus]. [žiūrėta 2019 m. balandžio 15 d.]. Prieiga per internetą: <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx>
 39. Bjorn, A. G. CORAS, A Platform for Risk Analysis on Security Critical Systems — Model-based Risk Analysis Targeting Security, International Conference on Telemedicine 2002 (ICT2002) [interaktyvus]. Regenburgas, 2002. [žiūrėta 2019 m. balandžio 4 d.]. Prieiga per internetą: <http://www.ewics.org/attachments/security-subgroup-boppard-2002/CORAS+framework.pdf>
 40. CORAS Tool 2.0 programinės įrangos paketai [interaktyvus]. [žiūrėta 2019 m. balandžio 4 d.]. Prieiga per internetą: <https://coras.sourceforge.net>
 41. Model Based Security Risk Analysis for Web Applications: The CORAS Approach [interaktyvus]. EuroWeb, 2002. [žiūrėta 2019 m. balandžio 4 d.]. Prieiga per internetą: https://www.researchgate.net/publication/266452327_Model-based_risk_assessment_-_the_CORAS_approach
 42. Alberts C. J.; Dorofee A. J. OCTAVE Method Implementation Guide Version 2.0 [interaktyvus]. Carnegie Mellon University, 2001. [žiūrėta 2019 m. balandžio 7 d.]. Prieiga per internetą: <https://www.cert.org/octave/omig.html>
 43. Alberts, C. J. ; Dorofee, A. J. 2002. Managing Information Security Risks — The OCTAVE Approach. Boston: Addison Wesley. ISBN 0-321-11886-3.
 44. CRAMM Expert Walkthrough and Overview [interaktyvus]. Insight Consulting, 2003. [žiūrėta 2019 m. balandžio 7 d.]. Prieiga per internetą: https://www.researchgate.net/publication/266452327_Model-based_risk_assessment_-_the_CORAS_approach

Priedai

1 PRIEDAS. Rizikos vertinimo metodikų charakteristikos

Rizikos sistemų charakteristikos	CORAS	OCTAVE	CRAMM
Bendros charakteristikos			
Pritaikymas įvairaus dydžio organizacijoms	Taip	Taip	Taip
Ataskaitų aiškumas	Taip	Taip	Ne
Taikymo patogumas	Taip	Taip	Taip
Prieinamumas	Taip	Taip	Ne
Palaikymas	Taip	Taip	Ne
Kiekybinis vertinimas	Taip	Taip	Taip
Kokybinis vertinimas	Taip	Taip	Taip
Plati grėsmių bazė	Ne	Ne	Taip
Informacijos teikimo personalui plėtra	Ne	Ne	Ne
Tinkamumas reguliariam taikymui	Ne	Taip	Taip
Nepriklausomas vertinimas	Taip	Ne	Taip
Pradinių duomenų nustatymas			
Turtas	Taip	Taip	Taip
Turto vertė	Taip	Taip	Taip
IT sistemų tipai	Taip	Taip	Taip
Pažeidžiamumas	Taip	Taip	Taip
Atsakomosios priemonės	Ne	Ne	Taip
Baziniai saugumo reikalavimai	Ne	Ne	Ne
Nuostolių tendencija	Ne	Ne	Ne
Saugos priemonės	Taip	Taip	Ne
Grėsmių dažnis	Ne	Ne	Ne
Tinklo įranga	Taip	Ne	Ne
Informacijos pobūdis	Ne	Ne	Ne
Vartotojų grupės	Ne	Ne	Ne
Apsaugos sistemos	Ne	Taip	Ne
Rizika			
Rizikos kategorijų taikymas	Taip	Taip	Taip
Leistinos rizikos sąvoka	Taip	Taip	Taip
Rizikos mažinimo planavimas	Taip	Taip	Taip
Valdymas			
Rizikos savininko nustatymas	Taip	Taip	Taip
Rizikos mažinimas	Taip	Taip	Taip
Seminarai ir susirinkimai	Ne	Taip	Ne
Verslo/IT rizikos vertinimas	Ne	Taip	Taip
Techninio lygio rizikos vertinimas	Taip	Ne	Taip
Organizacinio lygio rizikos vertinimas	Taip	Taip	Taip
Perspėjimas dėl galimų rizikų	Taip	Taip	Taip
Rizikos išvengimas	Ne	Ne	Taip
Rizikos priėmimas	Taip	Taip	Taip
Procesai			
Rizikos veiksniai			

Materialus turtas	Taip	Taip	Taip
Nematerialus turtas	Taip	Taip	Taip
Grėsmės	Taip	Taip	Taip
Turto vertė	Taip	Taip	Taip
Pažeidžiamumas	Taip	Taip	Taip
Saugos priemonės	Taip	Taip	Ne
Nuostoliai	Taip	Taip	Taip
Rizikos realizavimo tikimybė	Taip	Taip	Taip
Rizikos vertinimo rodikliai			
Kokybinis rodiklis	Taip	Taip	Taip
Kiekybinis rodiklis	Taip	Ne	Taip
Rizikos valdymo būdai			
Kokybinis rizikų išdėstymas	Taip	Taip	Taip
Kiekybinis rizikų išdėstymas	Taip	Ne	Taip
Nepriklausomas vertinimas	Taip	Ne	Taip
Investicijų grąžos skaičiavimas	Ne	Ne	Ne
Optimalaus balanso skaičiavimas:			
Prevencijos priemonėms	Taip	Ne	Ne
Identifikacijos priemonėms	Taip	Ne	Ne
Taisymo priemonėms	Taip	Ne	Ne
Atstatymo priemonėms	Taip	Taip	Ne
Valdymo būdų integracija	Ne	Ne	Ne
Valdymo būdų paskirties aprašymai	Ne	Taip	Taip
Likutinės rizikos priėmimas	Taip	Taip	Ne
Likutinės rizikos valdymas	Ne	Ne	Ne
Rizikų stebėjimas			
Rizikos prevencijos priemonių efektyvumo stebėjimas	Ne	Ne	Ne
Reagavimas į IT incidentus	Ne	Taip	Ne
Rizikos vertinimo rezultatų struktūrizuotas dokumentavimas	Taip	Taip	Ne

2 PRIEDAS. ISO/IEC 27005 PRIEDAS „C“ – TIPINIŲ GRĖSMIŲ PAVYZDŽIAI

Lentelėje C.1 pateikti tipinių grėsmių pavyzdžiai. Šis sąrašas naudojamas grėsmėms įvertinti. Grėsmės gali būti tyčinės, atsitiktinės arba susijusios su aplinkos poveikiu. Jų pasekmės – nuostolis arba reikiamų servisų praradimas. Kitas sąrašas nurodo grėsmių tinkamumą kiekvienam tipui, kur „D“ – tyčinės, „A“ – atsitiktinės, „E“ – ekologinės. „D“ tipas naudojamas visoms tyčinėms veikoms, kurių tikslas – informacinis turtas. „A“ tipas naudojamas visiems žmogiškiems veiksniams, kurie gali pažeisti informacinį turtą. „E“ tipas naudojamas visiems ne žmogaus veiksams, sukeliantiems incidentus. Grėsmių grupės išvardintos ne prioritetine tvarka.

Tipas	Grėsmės	Žymės
Fizinis pažeidimas	Ugnis	A, D, E
	Vanduo	A, D, E
	Užteršimas	A, D, E
	Incidentas	A, D, E
	Įrangos arba duomenų laikmenų sunaikinimas	A, D, E
	Dulkių, korozijos, šalčio poveikis	A, D, E
Natūralūs procesai	Klimato reiškiniai	E
	Seisminiai reiškiniai	E
	Vulkaniniai reiškiniai	E
	Meteorologiniai reiškiniai	E
	Potvyniai	E
Reikalingų servisų praradimas	Kondicionavimo arba vandens tiekimo sutrikimai	A, D
	Elektros tiekimo sutrikimai	A, D, E
	Telekomunikacinės įrangos sutrikimai	A, D
Sutrikimai dėl spinduliuotės poveikio	Elektromagnetinė spinduliuotė	A, D, E
	Šiluminė spinduliuotė	A, D, E
	Elektromagnetinis impulsas	A, D, E
Informacijos kompromitavimas	Kompromituoto signalo perėmimas ir siuntimas	D
	Nuotolinis šnipinėjimas	D
	Pokalbių klausymas	D
	Laikmenų ar dokumentų vagystė	D
	Įrangos vagystė	D
	Sugadintų ir/ar utilizuoti pateiktų laikmenų duomenų atkūrimas	D
	Identifikavimas (išslaptinimas)	A, D
	Nepatikimų šaltinių duomenys	A, D
	Aparatinės įrangos trikdymas	D
	Programinės įrangos trikdymas	D
	Geografinės padėties nustatymas	D
Techniniai sutrikimai	Įrangos gedimai	A
	Įrangos sutrikimai	A
	Informacinės sistemos įsotinimas	A, D
	Programiniai sutrikimai	A
	Įrangos pataisomumo pažeidimas	A, D
Neteisėti veiksmai	Neteisėtas įrangos panaudojimas	D
	Apgaulingas programinės įrangos kopijavimas	D
	Nelicencijuotos arba nukopijuotos programinės įrangos naudojimas	A, D
	Duomenų klastojimas	D
	Neteisėtas duomenų apdorojimas	D
	Naudojimo klaida	A

Funkcijų kompromitavimas	Piktnaudžiavimas teisėmis	A, D
	Teisių falsifikavimas	D
	Veiksmų neigimas	D
	Personalo veiksmingumo pažeidimas	A, D, E

Atskiras dėmesys turi būti skiriamas grėsmėms, kurių šaltinis – žmogus. Tokios grėsmės pateiktos šioje lentelėje:

Grėsmės šaltinis	Motyvacija	Galimos pasekmės
Įsilaužėlis („hakeris“)	Sukilimas Ego Iššūkis Statusas Pinigai	• Įsilaužimas • Socialinė inžinerija • Įsiskverbimas į sistemą, jos nulaužimas • Neteisėta prieiga prie sistemos
Kompiuterinis nusikaltėlis	Informacijos sunaikinimas Neteisėtas informacijos panaudojimas Finansinė arba kreditinė nauda Neteisėtas duomenų suklastojimas	• Kompiuteriniai nusikaltimai (pavyzdžiui, kibernetinis sekimas) • Sukčiavimo veiksmai (pavyzdžiui, paleidimas, pakartojimas, perėmimas) • Informacinis papirkimas • Imitacija • Įsilaužimas į sistemą
Teroristas	Kerštas Šnipinėjimas Sunaikinimas Šantažas Politinė nauda Paviešinimas žiniasklaidoje	• Sprogimas / teroristinis aktas • Informacinis karas • Sisteminė ataka (pavyzdžiui, paskirstyto aptarnavimo atsisakymas) • Įsilaužimas į sistemą • Sistemos trikdymas
Industrinis šnipinėjimas (kompanijos, užsienio vyriausybės, kiti vyriausybinių interesai)	Konkurencinis pranašumas Ekonominis šnipinėjimas	• Ekonominis šnipinėjimas • Informacinė vagystė • Asmens duomenų vagystė • Socialinė inžinerija (privatumo pažeidimas) • Įsilaužimas į sistemą • Neteisėta prieiga prie sistemos (prieiga prie konfidencialios, asmeninės arba technologinės informacijos)
Darbuotojas (blogai apmokytas, nepatenkintas, piktybiškai nusiteikęs, aplaidus, nesąžiningas, atleistas darbuotojas)	Šnipinėjimas Ego Smalsumas Finansinė nauda Kerštas Netyčinės klaidos arba jų nepastebėjimas (pavyzdžiui, duomenų įvedimo arba programavimo klaida)	• Darbuotojo užpuolimas • Šnipinėjimas • Įmonės paslapties peržiūra • Netinkamas kompiuterio naudojimas • Informacinis papirkimas • Falsifikuotų duomenų įvedimas, duomenų sunaikinimas • Perėmimas • Kenkėjiškas kodas (pavyzdžiui, virusas, „loginė bomba“, „Trojos arklys“) • Asmens duomenų pardavimas • Sisteminės klaidos • Įsilaužimas į sistemą • Sisteminis sabotažas • Neteisėta prieiga prie sistemos

3 PRIEDAS. ISO/IEC 27005 PRIEDO DALIS „D“ – PAŽEIDŽIAMUMAI

Lentelėje D.1 pateikti įvairių saugos sričių pažeidžiamumų pavyzdžiai, įskaitant grėsmių pavyzdžius, kuriais naudojantis galima išnaudoti išvardintus pažeidžiamumus. Šie sąrašai gali būti naudingi grėsmių ir pažeidžiamumų įvertinimo metu, nustatant prasmingų incidentų scenarijus. Verta paminėti, kad tam tikru atveju šie pažeidžiamumai gali būti panaudojami esant kitoms grėsmėms.

Tipas	Pažeidžiamumų pavyzdžiai	Grėsmių pavyzdžiai
Aparatinės priemonės	Nepakankamas aptarnavimas / diegimo defektas naudojant duomenų laikmenas	Įrangos pataisomumo pažeidimas
	Periodiškai keičiamų schemų trūkumai	Įrangos arba laikmenų sunaikinimas
	Jautrumas drėgmei, dulkėms, purvui	Dulkių, korozijos, šalčio poveikis
	Jautrumas elektromagnetinei radiacijai	Elektromagnetinė radiacija
	Efektyvios konfigūracijos pokyčių kontrolės trūkumai	Naudojimo klaida
	Jautrumas įtampos šuoliams	Elektros tiekimo sutrikimai
	Jautrumas temperatūros pokyčiui	Meteorologiniai reiškiniai
	Nepatikimas saugojimas	Laikmenų arba dokumentų vagystė
	Atsargumo stoka naikinant duomenis	Laikmenų arba dokumentų vagystė
	Neribojamas kopijavimas	Laikmenų arba dokumentų vagystė
Programinė įranga	Nepakankamas programinis testavimas	Piktnaudžiavimas teisėmis
	Žinomi programinės įrangos trūkumai	Piktnaudžiavimas teisėmis
	„Išėjimo iš sistemos“ nenaudojimas paliekant darbo stotį	Piktnaudžiavimas teisėmis
	Duomenų laikmenų perdavimas arba dažnas naudojimas tinkamai neištrinant duomenų	Piktnaudžiavimas teisėmis
	Mažas revizijų kiekis	Piktnaudžiavimas teisėmis
	Neteisingas prieigos teisių paskirstymas	Piktnaudžiavimas teisėmis
	Platus programinės įrangos taikymas	Duomenų klastojimas
	Taikomųjų programų naudojimas falsifikuotiems duomenims tam tikram terminui	Duomenų klastojimas
	Komplikuota vartotojo aplinka	Naudojimo klaida
	Dokumentacijos trūkumai	Naudojimo klaida
	Neteisingų parametrų nustatymas	Naudojimo klaida
	Nekorektiška data	Naudojimo klaida
Tinklas	Vartotojų autentifikavimo identifikuojančių ir aptinkančių algoritmų trūkumai	Teisių falsifikavimas
	Neapsaugotos slaptažodžių lentelės	Teisių falsifikavimas
	Blogas slaptažodžių valdymas	Teisių falsifikavimas
	Paleistos nereikalingos tarnybos	Neteisėtas duomenų apdorojimas
	Turinti trūkumų arba nauja programinė įranga	Programiniai sutrikimai
	Neišsamios, kūrėjams neaiškios specifikacijos	Programiniai sutrikimai
	Efektyvios konfigūracijos pokyčių kontrolės trūkumai	Programiniai sutrikimai
	Nevaldomas paleidimas ir programinės įrangos naudojimas	Programinės įrangos klastojimas
	Atsarginio kopijavimo proceso trūkumai	Programinės įrangos klastojimas
	Pastatų, durų, langų fizinės saugos trūkumai	Laikmenų ar dokumentų vagystė

	Ataskaitų patikros valdymo trūkumai	Neteisėtas įrangos panaudojimas
	Pranešimo gavimo įrodymų trūkumas	Veiksmų neigimas
	Neapsaugotos ryšio linijos	Pokalbių klausimas
	Neapsaugotas jautrus duomenų perdavimo srautas	Pokalbių klausimas
	Netinkama elektros instaliacija	Telekomunikacinės įrangos sutrikimai
	Vienintelis gedimo mazgas	Telekomunikacinės įrangos sutrikimai
	Siuntėjo ir gavėjo identifikacijos ir autentifikavimo trūkumai	Teisių falsifikavimas
	Pavojinga tinklo architektūra	Nuotolinis šnipinėjimas
	Atviras slaptažodžių perdavimas	Nuotolinis šnipinėjimas
	Netinkamas tinklo valdymas (sistemos gebėjimas atlaikyti komutacijos klaidas)	Informacinės sistemos įsotinimas
	Neapsaugotas prisijungimas prie bendro tinklo	Neteisėtas įrangos naudojimas
Personalias	Personalo trūkumas	Personalo veiksmingumo pažeidimas
	Neteisingas apmokymo procesas	Įrangos arba laikmenų sunaikinimas
	Nepakankamas saugos apmokymas	Naudojimo klaida
	Netinkamas programinės ir kompiuterinės įrangos naudojimas	Naudojimo klaida
	Saugumo supratimo trūkumai	Naudojimo klaida
	Stebėjimo mechanizmų trūkumas	Neteisėtas duomenų apdorojimas
	Išorės ir tvarkymo personalo nekontroliuojamas darbas	Laikmenų arba dokumentų vagystė
	Teisingo duomenų perdavimo laikmenų naudojimo ir pranešimų perdavimo politikos trūkumai	Neteisėtas įrangos panaudojimas
Tinklapis (organizacijos funkcionavimo vieta)	Neteisingas ir neatsargus fizinės pastato prieigos valdymo įrangos naudojimas	Įrangos arba laikmenų sunaikinimas
	Geografinė padėtis potvynio zonoje	Nestabilus tinklo galingumas
	Potvynis	Elektros tiekimo sutrikimai
	Pastatų, durų, langų fizinės saugos trūkumai	Piktnaudžiavimas teisėmis
	Formalaus vartotojų įregistravimo ir išregistravimo proceso trūkumai	Laikmenų arba dokumentų vagystė
	Formalios prieigos teisių peržiūros trūkumai (išsiuntimo valdymas)	Piktnaudžiavimas teisėmis
	Sąlygų trūkumas klientų bei trečiųjų šalių sutartyse	Piktnaudžiavimas teisėmis
	Duomenų apdorojimo valdymo proceso trūkumai	Piktnaudžiavimas teisėmis
	Reguliarių patikrų trūkumai (išsiuntimo valdymas)	Piktnaudžiavimas teisėmis
	Rizikos identifikavimo ir vertinimo procesų trūkumas	Piktnaudžiavimas teisėmis
	Ataskaitos įrašų dėl gedimų administratoriaus ir vartotojų žurnale informacijos trūkumas	Piktnaudžiavimas teisėmis

Netinkamas aptarnaujančiojo personalo grįžtamasis ryšys	Įrangos pataisomumo pažeidimas
Serviso aptarnavimo trūkumas ar nepakankama priežiūra	Įrangos pataisomumo pažeidimas
Pokyčių kontrolės proceso trūkumai	Įrangos pataisomumo pažeidimas
ISVS dokumentacijos valdymo proceso trūkumai	Duomenų klastojimas
ISVS įrašų, kurie formuoja išsiuntimo valdymą, formalių procesų trūkumai	Duomenų klastojimas
Bendrai naudojamos informacijos proceso formalaus leidimo trūkumai	Nepatikimų šaltinių duomenys
Tinkamo informacijos saugumo pareigų skirstymo trūkumai	Veiksmų neigimas
Tęstinumo planų trūkumai	Įrangos gedimai
El. pašto naudojimo politikos trūkumai	Naudojimo klaida
Procesų trūkumas siekiant įdiegti programinę įrangą į eksploatuojamas sistemas	Naudojimo klaida
Administratorių ir operatorių ataskaitų trūkumas registracijos failuose	Naudojimo klaida
Konfidencialių duomenų apdorojimo procesų trūkumas	Naudojimo klaida
Informacijos saugumo pareigų trūkumai uždavinių aprašymuose	Naudojimo klaida
Sąlygų deficitas ar trūkumai (informacijos saugos atžvilgiu) darbuotojų sutartyse	Neteisėtas duomenų apdorojimas
Tam tikro disciplininio proceso trūkumas informacijos saugos incidento atveju	Įrangos vagystė
Mobilios ir kompiuterinės technikos formalios naudojimo politikos trūkumas	Įrangos vagystė
Nuotolinės rezervacijos turto valdymo trūkumas	Įrangos vagystė
„Švaraus stalo ir švaraus ekrano“ politikos stygius	Laikmenų ar dokumentų vagystė
Informacijos apdorojimo priemonių sankcijų stygius	Laikmenų ar dokumentų vagystė
Įdiegtų valdymo mechanizmų saugos taisyklių pažeidimo atveju stygius	Laikmenų ar dokumentų vagystė
Reguliarios kontrolės (priežiūros) trūkumas	Neteisėtas įrangos panaudojimas
Pranešimų apie esamus saugos pažeidžiamumus trūkumas	Neteisėtas įrangos panaudojimas
Intelektualios nuosavybės sąlygų suderinimo procesų trūkumas	Nelicencijuotos ar nukopijuotos programinės įrangos naudojimas

4 PRIEDAS. PAŽEIDŽIAMUMŲ NUSTATYMO FORMA

Tipas	Pažeidžiamumų pavyzdžiai	Rizikų numeriai / kiekis															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Aparatinės priemonės	Nepakankamas aptarnavimas / diegimo defektas naudojant duomenų laikmenas	A	X	X		X	X		X	X	X		X		X		X
	Periodiškai keičiamų schemų trūkumai	B	X	X		X											
	Jautrumas drėgmei, dulkėms, purvui	C			X												
	Jautrumas elektromagnetinei radiacijai	D															
	Efekttyvios konfigūracijos pokyčių kontrolės trūkumai	E															
	Jautrumas įtampos šuoliams	F	X	X		X	X		X	X	X	X	X	X	X		
	Jautrumas temperatūros pokyčiui	G															
	Nepatikimas saugojimas	H				X			X	X	X	X	X	X	X		
	Atsargumo stoka naikinant duomenis	H															
	Neribojamas kopijavimas	H	X			X			X	X	X	X	X	X	X	X	X
	Nepakankamas programinis testavimas	I															
	Žinomi programinės įrangos trūkumai	I	X	X			X		X	X	X	X	X	X	X		
	„Išėjimo iš sistemos“ nenaudojimas paliekant darbo stotį	I						X									
	Duomenų laikmenų perdavimas arba dažnas naudojimas tinkamai neištrinant duomenų	I	X						X		X		X		X		
	Mažas revizių kiekis	I															
Programinė įranga	Neteisingas priteigos teisių paskirstymas	I	X	X	X			X	X		X		X		X		
	Platus programinės įrangos taikymas	J						X									
	Taikomųjų programų naudojimas falsifikuotiems duomenims tam tikram terminui	J															
	Komplikuota vartotojo aplinka	E	X	X			X	X	X			X					
	Dokumentacijos trūkumai	E															
	Neteisingų parametrų nustatymas	E				X		X	X		X		X				
	Nekorektiška data	E						X									
	Vartotojų autentifikaciją identifikuojančių ir aplinkančių algoritimų trūkumai	R	X			X										X	
	Neapsaugotos slaptažodžių lentelės	K							X	X	X		X		X		
	Blogas slaptažodžių valdymas	K						X									
	Paleistos nereikalingos tarnybos	L						X									
	Turinti trūkumų arba nauja programinė įranga	M	X	X			X	X		X		X		X			
	Neaiškios arba nepilnos specifikacijos kūrėjams	M				X											
	Efekttyvios konfigūracijos pokyčių kontrolės trūkumai	M								X		X		X			
	Nevaldomas paleidimas ir programinės įrangos naudojimas	N								X		X		X			
Tinklas	Atsarginio kopijavimo proceso trūkumai	N	X						X		X		X		X		X
	Pastatų, durų, langų fizinės saugos trūkumai	H	X	X							X		X		X		
	Ataskaitų patikros valdymo trūkumai	O															
	Pranešimo gavimo įrodymų trūkumas	P						X									
	Neapsaugotos ryšio linijos	Q				X										X	
	Neapsaugotas jautrus duomenų perdavimo srautas	Q							X		X		X		X	X	
	Netinkama elektros instaliacija	R		X													
	Vienintelis gedimo mazgas	R															
	Siuntėjo ir gavėjo identifikacijos ir autentifikacijos trūkumai	K															
	Pavojinga tinklo architektūra	S															
	Aviras slaptažodžių perdavimas	S	X						X		X		X		X	X	X
	Netinkamas tinklo valdymas (sistemos gebėjimas atlaikyti komutacijos klaidas)	T															
	Neapsaugotas prisijungimas prie bendro tinklo	O									X		X		X	X	
	Personalo trūkumas	U															
	Neteisingas apmokymo procesas	B															

5 PRIEDAS. GRĖSMIŲ NUSTATYMAS

Grėsmės		Nustatytos rizikos Nr.															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Įrangos pataisomumo pažeidimas		A	X	X	X	X	X		X	X	X	X	X	X	X		X
Įrangos ar laikmenų sunaikinimas		B	X	X		X											
Dulkių, korozijos, šalčio poveikis		C			X												
Elektromagnetinė radiacija		D															
Naudojimosi klaida		E	X	X	X	X	X		X	X	X	X	X	X	X		
Elektros tiekimo sutrikimai		F	X	X		X	X		X	X	X	X	X	X	X		
Meteorologiniai reiškiniai		G			X												
Laikmenų ar dokumentų vagystė		H	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Piktnaudžiavimas teisėmis		I	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Duomenų klastojimas		J					X									X	X
Teisių falsifikavimas		K					X	X	X	X	X	X	X	X	X		
Neteisėtas duomenų apdorojimas		L			X		X										
Programiniai sutrikimai		M	X	X		X	X	X	X			X		X			
Programinės įrangos klastojimas		N	X		X			X	X	X	X	X	X	X			X
Neteisėtas įrangos panaudojimas		O				X		X	X	X	X	X	X	X	X		
Veiksmų neįgyvendinimas		P					X									X	
Pokalbių klausymas		Q				X			X		X	X	X	X	X	X	
Telekomunikacinės įrangos sutrikimai		R	X	X												X	
Nuotolinis šnipinėjimas		S	X					X			X	X	X	X	X	X	X
Informacinės sistemos įsotinimas		T															
Personalo veiksmingumo pažeidimas		U															
Nestabilus tinklo galimumas		V															
Nepatikimų šaltinių duomenys		W															X
Įrangos gedimai		X	X	X			X	X		X				X		X	X
Įrangos vagystė		Y	X														X
Nelicencijuotos ar nukopijuotos programinės įrangos naudojimas		Z															X
Viso grėsmių:		12	9	7	7	7	6	9	10	10	9	12	9	12	9	11	5

6 PRIEDAS. APKLAUSOS ANKETA

1. Gamybiniai procesai			
Nr.	Klausimas	Technologijos valdymo sutrikimas	Technologijos stebėjimo sutrikimas
Informacinės sistemos kritiškumas			
1.	Interneto ryšio prieinamumas	A. Taip B. Ne	A. Taip B. Ne
2.	Duomenų perdavimo ryšys	A. Išorinis tinklas B. Vietinis tinklas	A. Išorinis tinklas B. Vietinis tinklas
3.	Naudojama kompiuterinės įrangos infrastruktūra	A. Fiziniai serveriai B. Virtualūs serveriai C. Personaliniai kompiuteriai D. Automatizuotos darbo vietos	A. Fiziniai serveriai B. Virtualūs serveriai C. Personaliniai kompiuteriai D. Automatizuotos darbo vietos
4.	Sistemos tipas	A. Uždaroji sistema, atliekanti apsaugos ir įvykių analizės funkcijas B. Tarnybinė stotis, kaupianti ir apdorojanti duomenys C. Palaikymo sistema, vizualizuojanti duomenis D. Atviroji sistema (tinklapis, informacinis žiniatinklis)	A. Uždaroji sistema, atliekanti apsaugos ir įvykių analizės funkcijas B. Tarnybinė stotis, kaupianti ir apdorojanti duomenys C. Palaikymo sistema, vizualizuojanti duomenis D. Atviroji sistema (tinklapis, informacinis žiniatinklis)
Procesų pažeidžiamumo lygis			
5.	IT infrastruktūros procesų funkcija	A. Užtikrina kelių procesų veiklą B. Užtikrina vieno proceso veiklą C. Užtikrina procesų palaikymą D. Neįtakoja procesų veiklos	A. Užtikrina kelių procesų veiklą B. Užtikrina vieno proceso veiklą C. Užtikrina procesų palaikymą D. Neįtakoja procesų veiklos
6.	IT infrastruktūros funkcijos sutrikimo įtaka procesams	A. Sustabdo kelių procesų veiklą B. Sustabdo vieno proceso veiklą C. Sulėtina procesų veiklą D. Neįtakoja procesų	A. Sustabdo kelių procesų veiklą B. Sustabdo vieno proceso veiklą C. Sulėtina procesų veiklą D. Neįtakoja procesų
Organizacijos veiklos reguliavimas			
7.	Proceso reguliavimo būdai	A. Atsitiktiniu metu vykdomas komisijos patikrinimas B. Reguliarus auditas C. Vidinės/tarnybinės patikros D. Nevyksta reguliavimo procedūros	A. Atsitiktiniu metu vykdomas komisijos patikrinimas B. Reguliarus auditas C. Vidinės/tarnybinės patikros D. Nevyksta reguliavimo procedūros
8.	Incidento įtaka proceso reguliavimui	A. Skiriamos baudos B. Padidinamas auditorių dėmesys C. Gaunami nurodymai be baudžiamųjų sankcijų D. Niekas nevyksta	A. Skiriamos baudos B. Padidinamas auditorių dėmesys C. Gaunami nurodymai be baudžiamųjų sankcijų D. Niekas nevyksta
Reputacijos lygis			
9.	Įtaka įmonės reputacijai	A. Reputacija pažeminama tautiniu lygmeniu B. Reputacija pažeminama regioniniu lygmeniu C. Reputacija pažeminama internete D. Reputacija nepažeminama	A. Reputacija pažeminama tautiniu lygmeniu B. Reputacija pažeminama regioniniu lygmeniu C. Reputacija pažeminama internete D. Reputacija nepažeminama
Grėsmės arba pažeidžiamumo išnaudojimo asmenų potencialas			
10.	Kas turi prieigą prie IT infrastruktūros	A. Techninės priežiūros personalas (IT darbuotojai) B. Aptarnaujantis personalas (specialistai, operatoriai) C. Tretieji asmenys D. Nekvalifikuoti darbuotojai	A. Techninės priežiūros personalas (IT darbuotojai) B. Aptarnaujantis personalas (specialistai, operatoriai) C. Tretieji asmenys D. Nekvalifikuoti darbuotojai
11.	Kas atlieka duomenų operavimo funkciją	A. Techninės priežiūros personalas B. Kvalifikuoti vartotojai C. Nekvalifikuoti vartotojai D. Duomenimis nėra operuojama rankiniu būdu	A. Techninės priežiūros personalas B. Kvalifikuoti vartotojai C. Nekvalifikuoti vartotojai D. Duomenimis nėra operuojama rankiniu būdu
Taikomų prevencijos priemonių efektyvumas			
12.	Taikomos prevencijos priemonės	A. Apsaugos įranga nuo neteisėto įsibrovimo į įmonės tinklą B. Kenkėjiškų programų aptikimo programinė įranga C. Tinklo skirstymo priemonės D. VPN priemonės E. Virtualizavimo priemonių apsauga F. Neteisėto įsibrovimo į įmonės tinklą aptikimo įranga G. Apsaugos analizės priemonės	A. Apsaugos įranga nuo neteisėto įsibrovimo į įmonės tinklą B. Kenkėjiškų programų aptikimo programinė įranga C. Tinklo skirstymo priemonės D. VPN priemonės E. Virtualizavimo priemonių apsauga F. Neteisėto įsibrovimo į įmonės tinklą aptikimo įranga G. Apsaugos analizės priemonės

2. Laboratoriniai procesai			
Nr.	Klausimas	Laboratorijos veiklos sutrikimas	Laboratorijos duomenų praradimas / suklustojimas
Informacinės sistemos kritiškumas			
1.	Interneto ryšio prieinamumas	A. Taip B. Ne	A. Taip B. Ne
2.	Duomenų perdavimo ryšys	A. Išorinis tinklas B. Vietinis tinklas	A. Išorinis tinklas B. Vietinis tinklas
3.	Naudojama kompiuterinės įrangos infrastruktūra	A. Fiziniai serveriai B. Virtūalus serveriai C. Personaliniai kompiuteriai D. Automatizuotos darbo vietos	A. Fiziniai serveriai B. Virtūalus serveriai C. Personaliniai kompiuteriai D. Automatizuotos darbo vietos
4.	Sistemos tipas	A. Uždaroji sistema, atliekanti apsaugos ir įvykių analizės funkcijas B. Tarnybinė stotis, kaupianti ir apdorojanti duomenys C. Palaikymo sistema, vizualizuojanti duomenis D. Atviroji sistema (tinklapis, informacinis žiniatinklis)	A. Uždaroji sistema, atliekanti apsaugos ir įvykių analizės funkcijas B. Tarnybinė stotis, kaupianti ir apdorojanti duomenys C. Palaikymo sistema, vizualizuojanti duomenis D. Atviroji sistema (tinklapis, informacinis žiniatinklis)
Procesų pažeidžiamumo lygis			
5.	IT infrastruktūros procesų funkcija	A. Užtikrina kelių procesų veiklą B. Užtikrina vieno proceso veiklą C. Užtikrina procesų palaikymą D. Neįtakoja procesų veiklos	A. Užtikrina kelių procesų veiklą B. Užtikrina vieno proceso veiklą C. Užtikrina procesų palaikymą D. Neįtakoja procesų veiklos
6.	IT infrastruktūros funkcijos sutrikimo įtaka procesams	A. Sustabdo kelių procesų veiklą B. Sustabdo vieno proceso veiklą C. Sulėtina procesų įgyvendinimą D. Neįtakoja procesų	A. Sustabdo kelių procesų veiklą B. Sustabdo vieno proceso veiklą C. Sulėtina procesų įgyvendinimą D. Neįtakoja procesų
Organizacijos veiklos reguliavimas			
7.	Proceso reguliavimo būdai	A. Atsitiktiniu metu vykdomas komisijos patikrinimas B. Reguliarus auditas C. Vidinės/tarnybinės patikros D. Nevyksta reguliavimo procedūros	A. Atsitiktiniu metu vykdomas komisijos patikrinimas B. Reguliarus auditas C. Vidinės/tarnybinės patikros D. Nevyksta reguliavimo procedūros
8.	Incidento įtaka proceso reguliavimui	A. Skiriamos baudos B. Padidinamas auditorių dėmesys C. Gaunami nurodymai be baudžiamųjų sankcijų D. Niekas nevyksta	A. Skiriamos baudos B. Padidinamas auditorių dėmesys C. Gaunami nurodymai be baudžiamųjų sankcijų D. Niekas nevyksta
Reputacijos lygis			
9.	Įtaka įmonės reputacijai	A. Reputacija pažeminama tautiniu lygmeniu B. Reputacija pažeminama regioniniu lygmeniu C. Reputacija pažeminama internete D. Reputacija nepažeminama	A. Reputacija pažeminama tautiniu lygmeniu B. Reputacija pažeminama regioniniu lygmeniu C. Reputacija pažeminama internete D. Reputacija nepažeminama
Grėsmės arba pažeidžiamumo išnaudojimo asmenų potencialas			
10.	Kas turi prieigą prie IT infrastruktūros	A. Techninės priežiūros personalas (IT darbuotojai) B. Aptarnaujantis personalas (specialistai, operatoriai) C. Tretieji asmenys D. Nekvalifikuoti darbuotojai	A. Techninės priežiūros personalas (IT darbuotojai) B. Aptarnaujantis personalas (specialistai, operatoriai) C. Tretieji asmenys D. Nekvalifikuoti darbuotojai
11.	Kas atlieka duomenų operavimo funkciją	A. Techninės priežiūros personalas B. Kvalifikuoti vartotojai C. Nekvalifikuoti vartotojai D. Duomenimis nėra operuojama rankiniu būdu	A. Techninės priežiūros personalas B. Kvalifikuoti vartotojai C. Nekvalifikuoti vartotojai D. Duomenimis nėra operuojama rankiniu būdu
Taikomų prevencijos priemonių efektyvumas			
12.	Taikomos prevencijos priemonės	A. Apsaugos įranga nuo neteisėto įsibrovimo į įmonės tinklą B. Kenkėjiškų programų aptikimo programinė įranga C. Tinklo skirstymo priemonės D. VPN priemonės E. Virtualizavimo priemonių apsauga F. Neteisėto įsibrovimo į įmonės tinklą aptikimo įranga G. Apsaugos analizės priemonės	A. Apsaugos įranga nuo neteisėto įsibrovimo į įmonės tinklą B. Kenkėjiškų programų aptikimo programinė įranga C. Tinklo skirstymo priemonės D. VPN priemonės E. Virtualizavimo priemonių apsauga F. Neteisėto įsibrovimo į įmonės tinklą aptikimo įranga G. Apsaugos analizės priemonės

3. Paslaugų tiekimo procesai			
Nr.	Klausimas	Paslaugų tiekimo valdymo sutrikimas	Paslaugų tiekimo stebėjimo sutrikimas
Informacinės sistemos kritiškumas			
1.	Interneto ryšio prieinamumas	A. Taip B. Ne	A. Taip B. Ne
2.	Duomenų perdavimo ryšys	A. Išorinis tinklas B. Vietinis tinklas	A. Išorinis tinklas B. Vietinis tinklas
3.	Naudojama kompiuterinės įrangos infrastruktūra	A. Fiziniai serveriai B. Virtualūs serveriai C. Personaliniai kompiuteriai D. Automatizuotos darbo vietos	A. Fiziniai serveriai B. Virtualūs serveriai C. Personaliniai kompiuteriai D. Automatizuotos darbo vietos
4.	Sistemos tipas	A. Uždaroji sistema, atliekanti apsaugos ir įvykių analizės funkcijas B. Tarnybinė stotis, kaupianti ir apdorojanti duomenys C. Palaikymo sistema, vizualizuojanti duomenis D. Atviroji sistema (tinklapis, informacinis žiniatinklis)	A. Uždaroji sistema, atliekanti apsaugos ir įvykių analizės funkcijas B. Tarnybinė stotis, kaupianti ir apdorojanti duomenys C. Palaikymo sistema, vizualizuojanti duomenis D. Atviroji sistema (tinklapis, informacinis žiniatinklis)
Procesų pažeidžiamumo lygis			
5.	IT infrastruktūros procesų funkcija	A. Užtikrina kelių procesų veiklą B. Užtikrina vieno proceso veiklą C. Užtikrina procesų palaikymą D. Neįtakoja procesų veiklos	A. Užtikrina kelių procesų veiklą B. Užtikrina vieno proceso veiklą C. Užtikrina procesų palaikymą D. Neįtakoja procesų veiklos
6.	IT infrastruktūros funkcijos sutrikimo įtaka procesams	A. Sustabdo kelių procesų veiklą B. Sustabdo vieno proceso veiklą C. Sulėtina procesų įgyvendinimą D. Neįtakoja procesų	A. Sustabdo kelių procesų veiklą B. Sustabdo vieno proceso veiklą C. Sulėtina procesų įgyvendinimą D. Neįtakoja procesų
Organizacijos veiklos reguliavimas			
7.	Procesas reguliuojamas	A. Atsitiktiniu metu vykdomas komisijos patikrinimas B. Reguliarus auditas C. Vidinės/tarnybinės patikros D. Nevyksta reguliavimo procedūros	A. Atsitiktiniu metu vykdomas komisijos patikrinimas B. Reguliarus auditas C. Vidinės/tarnybinės patikros D. Nevyksta reguliavimo procedūros
8.	Incidento įtaka proceso reguliavimui	A. Skiriamos baudos B. Padidinamas auditorių dėmesys C. Gaunami nurodymai be baudžiamųjų sankcijų D. Niekas nevyksta	A. Skiriamos baudos B. Padidinamas auditorių dėmesys C. Gaunami nurodymai be baudžiamųjų sankcijų D. Niekas nevyksta
Reputacijos lygis			
9.	Įtaka įmonės reputacijai	A. Reputacija pažeminama tautiniu lygmeniu B. Reputacija pažeminama regioniniu lygmeniu C. Reputacija pažeminama internete D. Reputacija nepažeminama	A. Reputacija pažeminama tautiniu lygmeniu B. Reputacija pažeminama regioniniu lygmeniu C. Reputacija pažeminama internete D. Reputacija nepažeminama
Grėsmės arba pažeidžiamumo išnaudojimo asmenų potencialas			
10.	Kas turi prieigą prie IT infrastruktūros	A. Techninės priežiūros personalas (IT darbuotojai) B. Aptarnaujantis personalas (specialistai, operatoriai) C. Tretieji asmenys D. Nekvalifikuoti darbuotojai	A. Techninės priežiūros personalas (IT darbuotojai) B. Aptarnaujantis personalas (specialistai, operatoriai) C. Tretieji asmenys D. Nekvalifikuoti darbuotojai
11.	Kas atlieka duomenų operavimo funkciją	A. Techninės priežiūros personalas B. Kvalifikuoti vartotojai C. Nekvalifikuoti vartotojai D. Duomenimis nėra operuojama rankiniu būdu	A. Techninės priežiūros personalas B. Kvalifikuoti vartotojai C. Nekvalifikuoti vartotojai D. Duomenimis nėra operuojama rankiniu būdu
Taikomų prevencijos priemonių efektyvumas			
12.	Taikomos prevencijos priemonės	A. Apsaugos įranga nuo neteisėto įsibrovimo į įmonės tinklą B. Kenkėjiškų programų aptikimo programinė įranga C. Tinklo skirstymo priemonės D. VPN priemonės E. Virtualizavimo priemonių apsauga F. Neteisėto įsibrovimo į įmonės tinklą aptikimo įranga G. Apsaugos analizės priemonės	A. Apsaugos įranga nuo neteisėto įsibrovimo į įmonės tinklą B. Kenkėjiškų programų aptikimo programinė įranga C. Tinklo skirstymo priemonės D. VPN priemonės E. Virtualizavimo priemonių apsauga F. Neteisėto įsibrovimo į įmonės tinklą aptikimo įranga G. Apsaugos analizės priemonės

4. Klientų aptarnavimo procesai			
Nr.	Klausimas	Klientų aptarnavimo procesų sutrikimas	Klientų duomenų nutekėjimas \ praradimas
Informacinės sistemos kritiškumas			
1.	Interneto ryšio prieinamumas	A. Taip B. Ne	A. Taip B. Ne
2.	Duomenų perdavimo ryšys	A. Išorinis tinklas C. Vietinis tinklas	A. Išorinis tinklas B. Vietinis tinklas
3.	Naudojama kompiuterinės įrangos infrastruktūra	A. Fiziniai serveriai B. Virtualūs serveriai C. Personaliniai kompiuteriai D. Automatizuotos darbo vietos	A. Fiziniai serveriai B. Virtualūs serveriai C. Personaliniai kompiuteriai D. Automatizuotos darbo vietos
4.	Sistemos tipas	A. Uždaroji sistema, atliekanti apsaugos ir įvykių analizės funkcijas B. Tarnybinė stotis, kaupianti ir apdorojanti duomenys C. Palaikymo sistema, vizualizuojanti duomenis D. Atviroji sistema (tinklapis, informacinis žiniatinklis)	A. Uždaroji sistema, atliekanti apsaugos ir įvykių analizės funkcijas B. Tarnybinė stotis, kaupianti ir apdorojanti duomenys C. Palaikymo sistema, vizualizuojanti duomenis D. Atviroji sistema (tinklapis, informacinis žiniatinklis)
Procesų pažeidžiamumo lygis			
5.	IT infrastruktūros procesų funkcija	A. Užtikrina kelių procesų veiklą B. Užtikrina vieno proceso veiklą C. Užtikrina procesų palaikymą D. Neįtakoja procesų veiklos	A. Užtikrina kelių procesų veiklą B. Užtikrina vieno proceso veiklą C. Užtikrina procesų palaikymą D. Neįtakoja procesų veiklos
6.	IT infrastruktūros funkcijos sutrikimo įtaka procesams	A. Sustabdo kelių procesų veiklą B. Sustabdo vieno proceso veiklą C. Sulėtina procesų įgyvendinimą D. Neįtakoja procesų	A. Sustabdo kelių procesų veiklą B. Sustabdo vieno proceso veiklą C. Sulėtina procesų įgyvendinimą D. Neįtakoja procesų
Organizacijos veiklos reguliavimas			
7.	Procesas reguliuojamas	A. Atsitiktiniu metu vykdomas komisijos patikrinimas B. Reguliarus auditas C. Vidinės/tarnybinės patikros D. Nevyksta reguliavimo procedūros	A. Atsitiktiniu metu vykdomas komisijos patikrinimas B. Reguliarus auditas C. Vidinės/tarnybinės patikros D. Nevyksta reguliavimo procedūros
8.	Incidento įtaka proceso reguliavimui	A. Skiriamos baudos B. Padidinamas auditorių dėmesys C. Gaunami nurodymai be baudžiamųjų sankcijų D. Niekas nevyksta	A. Skiriamos baudos B. Padidinamas auditorių dėmesys C. Gaunami nurodymai be baudžiamųjų sankcijų D. Niekas nevyksta
Reputacijos lygis			
9.	Įtaka įmonės reputacijai	A. Reputacija pažeminama tautiniu lygmeniu B. Reputacija pažeminama regioniniu lygmeniu C. Reputacija pažeminama internete D. Reputacija nepažeminama	A. Reputacija pažeminama tautiniu lygmeniu B. Reputacija pažeminama regioniniu lygmeniu C. Reputacija pažeminama internete D. Reputacija nepažeminama
Grėsmės arba pažeidžiamumo išnaudojimo asmenų potencialas			
10.	Kas turi prieigą prie IT infrastruktūros	A. Techninės priežiūros personalas (IT darbuotojai) B. Aptarnaujantis personalas (specialistai, operatoriai) C. Tretieji asmenys D. Nekvalifikuoti darbuotojai	A. Techninės priežiūros personalas (IT darbuotojai) B. Aptarnaujantis personalas (specialistai, operatoriai) C. Tretieji asmenys D. Nekvalifikuoti darbuotojai
11.	Kas atlieka duomenų operavimo funkciją	A. Techninės priežiūros personalas B. Kvalifikuoti vartotojai C. Nekvalifikuoti vartotojai D. Duomenimis nėra operuojama rankiniu būdu	A. Techninės priežiūros personalas B. Kvalifikuoti vartotojai C. Nekvalifikuoti vartotojai D. Duomenimis nėra operuojama rankiniu būdu
Taikomų prevencijos priemonių efektyvumas			
12.	Taikomos prevencijos priemonės	A. Apsaugos įranga nuo neteisėto įsibrovimo į įmonės tinklą B. Kenkėjiškų programų aptikimo programinė įranga C. Tinklo skirstymo priemonės D. VPN priemonės E. Virtualizavimo priemonių apsauga F. Neteisėto įsibrovimo į įmonės tinklą aptikimo įranga G. Apsaugos analizės priemonės	A. Apsaugos įranga nuo neteisėto įsibrovimo į įmonės tinklą B. Kenkėjiškų programų aptikimo programinė įranga C. Tinklo skirstymo priemonės D. VPN priemonės E. Virtualizavimo priemonių apsauga F. Neteisėto įsibrovimo į įmonės tinklą aptikimo įranga G. Apsaugos analizės priemonės

5. Vidaus resursų ir išteklių valdymo procesai			
Nr.	Klausimas	Finansų apskaitos valdymo procesų sutrikimas	Finansų apskaitos duomenų praradimas
Informacinės sistemos kritiškumas			
1.	Interneto ryšio prieinamumas	A. Taip B. Ne	A. Taip B. Ne
2.	Duomenų perdavimo ryšys	A. Išorinis tinklas B. Vietinis tinklas	A. Išorinis tinklas B. Vietinis tinklas
3.	Naudojama kompiuterinės įrangos infrastruktūra	A. Fiziniai serveriai B. Virtualūs serveriai C. Personaliniai kompiuteriai D. Automatizuotos darbo vietos	A. Fiziniai serveriai B. Virtualūs serveriai C. Personaliniai kompiuteriai D. Automatizuotos darbo vietos
4.	Sistemos tipas	A. Uždaroji sistema, atliekanti apsaugos ir įvykių analizės funkcijas B. Tarnybinė stotis, kaupianti ir apdorojanti duomenys C. Palaikymo sistema, vizualizuojanti duomenis D. Atviroji sistema (tinklapis, informacinis žiniatinklis)	A. Uždaroji sistema, atliekanti apsaugos ir įvykių analizės funkcijas B. Tarnybinė stotis, kaupianti ir apdorojanti duomenys C. Palaikymo sistema, vizualizuojanti duomenis D. Atviroji sistema (tinklapis, informacinis žiniatinklis)
Procesų pažeidžiamumo lygis			
5.	IT infrastruktūros procesų funkcija	A. Užtikrina kelių procesų veiklą B. Užtikrina vieno proceso veiklą C. Užtikrina procesų palaikymą D. Neįtakoja procesų veiklos	A. Užtikrina kelių procesų veiklą B. Užtikrina vieno proceso veiklą C. Užtikrina procesų palaikymą D. Neįtakoja procesų veiklos
6.	IT infrastruktūros funkcijos sutrikimo įtaka procesams	A. Sustabdo kelių procesų veiklą B. Sustabdo vieno proceso veiklą C. Sulėtina procesų įgyvendinimą D. Neįtakoja procesų	A. Sustabdo kelių procesų veiklą B. Sustabdo vieno proceso veiklą C. Sulėtina procesų įgyvendinimą D. Neįtakoja procesų
Organizacijos veiklos reguliavimas			
7.	Procesas reguliuojamas	A. Atsitiktiniu metu vykdomas komisijos patikrinimas B. Reguliarus auditas C. Vidinės/tarnybinės patikros D. Nevyksta reguliavimo procedūros	A. Atsitiktiniu metu vykdomas komisijos patikrinimas B. Reguliarus auditas C. Vidinės/tarnybinės patikros D. Nevyksta reguliavimo procedūros
8.	Incidento įtaka proceso reguliavimui	A. Skiriamos baudos B. Padidinamas auditorių dėmesys C. Gaunami nurodymai be baudžiamųjų sankcijų D. Niekas nevyksta	A. Skiriamos baudos B. Padidinamas auditorių dėmesys C. Gaunami nurodymai be baudžiamųjų sankcijų D. Niekas nevyksta
Reputacijos lygis			
9.	Įtaka įmonės reputacijai	A. Reputacija pažeminama tautiniu lygmeniu B. Reputacija pažeminama regioniniu lygmeniu C. Reputacija pažeminama internete D. Reputacija nepažeminama	A. Reputacija pažeminama tautiniu lygmeniu B. Reputacija pažeminama regioniniu lygmeniu C. Reputacija pažeminama internete D. Reputacija nepažeminama
Grėsmės arba pažeidžiamumo išnaudojimo asmenų potencialas			
10.	Kas turi prieigą prie IT infrastruktūros	A. Techninės priežiūros personalas (IT darbuotojai) B. Aptarnaujantis personalas (specialistai, operatoriai) C. Tretieji asmenys D. Nekvalifikuoti darbuotojai	A. Techninės priežiūros personalas (IT darbuotojai) B. Aptarnaujantis personalas (specialistai, operatoriai) C. Tretieji asmenys D. Nekvalifikuoti darbuotojai
11.	Kas atlieka duomenų operavimo funkciją	A. Techninės priežiūros personalas B. Kvalifikuoti vartotojai C. Nekvalifikuoti vartotojai D. Duomenimis nėra operuojama rankiniu būdu	A. Techninės priežiūros personalas B. Kvalifikuoti vartotojai C. Nekvalifikuoti vartotojai D. Duomenimis nėra operuojama rankiniu būdu
Taikomų prevencijos priemonių efektyvumas			
12.	Taikomos prevencijos priemonės	A. Apsaugos įranga nuo neteisėto įsibrovimo į įmonės tinklą B. Kenkėjiškų programų aptikimo programinė įranga C. Tinklo skirstymo priemonės D. VPN priemonės E. Virtualizavimo priemonių apsauga F. Neteisėto įsibrovimo į įmonės tinklą aptikimo įranga G. Apsaugos analizės priemonės	A. Apsaugos įranga nuo neteisėto įsibrovimo į įmonės tinklą B. Kenkėjiškų programų aptikimo programinė įranga C. Tinklo skirstymo priemonės D. VPN priemonės E. Virtualizavimo priemonių apsauga F. Neteisėto įsibrovimo į įmonės tinklą aptikimo įranga G. Apsaugos analizės priemonės

5.1. Vidaus resursų ir išteklių valdymo procesai			
Nr.	Klausimas	Atsargų ir išteklių valdymo procesų sutrikimas	Atsargų ir išteklių valdymo duomenų praradimas
Informacinės sistemos kritiškumas			
1.	Interneto ryšio prieinamumas	A. Taip B. Ne	A. Taip B. Ne
2.	Duomenų perdavimo ryšys	A. Išorinis tinklas B. Vietinis tinklas	A. Išorinis tinklas B. Vietinis tinklas
3.	Naudojama kompiuterinės įrangos infrastruktūra	A. Fiziniai serveriai B. Virtualūs serveriai C. Personaliniai kompiuteriai D. Automatizuotos darbo vietos	A. Fiziniai serveriai B. Virtualūs serveriai C. Personaliniai kompiuteriai D. Automatizuotos darbo vietos
4.	Sistemos tipas	A. Uždaroji sistema, atliekanti apsaugos ir įvykių analizės funkcijas B. Tarnybinė stotis, kaupianti ir apdorojanti duomenys C. Palaikymo sistema, vizualizuojanti duomenis D. Atviroji sistema (tinklapis, informacinis žiniatinklis)	A. Uždaroji sistema, atliekanti apsaugos ir įvykių analizės funkcijas B. Tarnybinė stotis, kaupianti ir apdorojanti duomenys C. Palaikymo sistema, vizualizuojanti duomenis D. Atviroji sistema (tinklapis, informacinis žiniatinklis)
Procesų pažeidžiamumo lygis			
5.	IT infrastruktūros procesų funkcija	A. Užtikrina kelių procesų veiklą B. Užtikrina vieno proceso veiklą C. Užtikrina procesų palaikymą D. Neįtakoja procesų veiklos	A. Užtikrina kelių procesų veiklą B. Užtikrina vieno proceso veiklą C. Užtikrina procesų palaikymą D. Neįtakoja procesų veiklos
6.	IT infrastruktūros funkcijos sutrikimo įtaka procesams	A. Sustabdo kelių procesų veiklą B. Sustabdo vieno proceso veiklą C. Sulėtina procesų įgyvendinimą D. Neįtakoja procesų	A. Sustabdo kelių procesų veiklą B. Sustabdo vieno proceso veiklą C. Sulėtina procesų įgyvendinimą D. Neįtakoja procesų
Organizacijos veiklos reguliavimas			
7.	Procesas reguliuojamas	A. Atsitiktiniu metu vykdomas komisijos patikrinimas B. Reguliarus auditas C. Vidinės/tarnybinės patikros D. Nevyksta reguliavimo procedūros	A. Atsitiktiniu metu vykdomas komisijos patikrinimas B. Reguliarus auditas C. Vidinės/tarnybinės patikros D. Nevyksta reguliavimo procedūros
8.	Incidento įtaka proceso reguliavimui	A. Skiriamos baudos B. Padidinamas auditorių dėmesys C. Gaunami nurodymai be baudžiamųjų sankcijų D. Niekas nevyksta	A. Skiriamos baudos B. Padidinamas auditorių dėmesys C. Gaunami nurodymai be baudžiamųjų sankcijų D. Niekas nevyksta
Reputacijos lygis			
9.	Įtaka įmonės reputacijai	A. Reputacija pažeminama tautiniu lygmeniu B. Reputacija pažeminama regioniniu lygmeniu C. Reputacija pažeminama internete D. Reputacija nepažeminama	A. Reputacija pažeminama tautiniu lygmeniu B. Reputacija pažeminama regioniniu lygmeniu C. Reputacija pažeminama internete D. Reputacija nepažeminama
Grėsmės arba pažeidžiamumo išnaudojimo asmenų potencialas			
10.	Kas turi prieigą prie IT infrastruktūros	A. Techninės priežiūros personalas (IT darbuotojai) B. Aptarnaujantis personalas (specialistai, operatoriai) C. Tretieji asmenys D. Nekvalifikuoti darbuotojai	A. Techninės priežiūros personalas (IT darbuotojai) B. Aptarnaujantis personalas (specialistai, operatoriai) C. Tretieji asmenys D. Nekvalifikuoti darbuotojai
11.	Kas atlieka duomenų operavimo funkciją	A. Techninės priežiūros personalas B. Kvalifikuoti vartotojai C. Nekvalifikuoti vartotojai D. Duomenimis nėra operuojama rankiniu būdu	A. Techninės priežiūros personalas B. Kvalifikuoti vartotojai C. Nekvalifikuoti vartotojai D. Duomenimis nėra operuojama rankiniu būdu
Taikomų prevencijos priemonių efektyvumas			
12.	Taikomos prevencijos priemonės	A. Apsaugos įranga nuo neteisėto įsibrovimo į įmonės tinklą B. Kenkėjiškų programų aptikimo programinė įranga C. Tinklo skirstymo priemonės D. VPN priemonės E. Virtualizavimo priemonių apsauga F. Neteisėto įsibrovimo į įmonės tinklą aptikimo įranga G. Apsaugos analizės priemonės	A. Apsaugos įranga nuo neteisėto įsibrovimo į įmonės tinklą B. Kenkėjiškų programų aptikimo programinė įranga C. Tinklo skirstymo priemonės D. VPN priemonės E. Virtualizavimo priemonių apsauga F. Neteisėto įsibrovimo į įmonės tinklą aptikimo įranga G. Apsaugos analizės priemonės

5.2. Vidaus resursų ir išteklių valdymo procesai			
Nr.	Klausimas	Personalo valdymo procesų sutrikimas	Personalo duomenų praradimas
Informacinės sistemos kritiškumams			
1.	Interneto ryšio prieinamumas	A. Taip B. Ne	A. Taip B. Ne
2.	Duomenų perdavimo ryšys	A. Išorinis tinklas B. Vietinis tinklas	A. Išorinis tinklas B. Vietinis tinklas
3.	Naudojama kompiuterinės įrangos infrastruktūra	A. Fiziniai serveriai B. Virtualūs serveriai C. Personaliniai kompiuteriai D. Automatizuotos darbo vietos	A. Fiziniai serveriai B. Virtualūs serveriai C. Personaliniai kompiuteriai D. Automatizuotos darbo vietos
4.	Sistemos tipas	A. Uždaroji sistema, atliekanti apsaugos ir įvykių analizės funkcijas B. Tarnybinė stotis, kaupianti ir apdorojanti duomenys C. Palaikymo sistema, vizualizuojanti duomenis D. Atviroji sistema (tinklapis, informacinis žiniatinklis)	A. Uždaroji sistema, atliekanti apsaugos ir įvykių analizės funkcijas B. Tarnybinė stotis, kaupianti ir apdorojanti duomenys C. Palaikymo sistema, vizualizuojanti duomenis D. Atviroji sistema (tinklapis, informacinis žiniatinklis)
Procesų pažeidžiamumo lygis			
5.	IT infrastruktūros procesų funkcija	A. Užtikrina kelių procesų veiklą B. Užtikrina vieno proceso veiklą C. Užtikrina procesų palaikymą D. Neįtakoja procesų veiklos	A. Užtikrina kelių procesų veiklą B. Užtikrina vieno proceso veiklą C. Užtikrina procesų palaikymą D. Neįtakoja procesų veiklos
6.	IT infrastruktūros funkcijos sutrikimo įtaka procesams	A. Sustabdo kelių procesų veiklą B. Sustabdo vieno proceso veiklą C. Sulėtina procesų įgyvendinimą D. Neįtakoja procesų	A. Sustabdo kelių procesų veiklą B. Sustabdo vieno proceso veiklą C. Sulėtina procesų įgyvendinimą D. Neįtakoja procesų
Organizacijos veiklos reguliavimas			
7.	Procesas reguliuojamas	A. Atsitiktiniu metu vykdomas komisijos patikrinimas B. Reguliarus auditas C. Vidinės/tarnybinės patikros D. Nevyksta reguliavimo procedūros	A. Atsitiktiniu metu vykdomas komisijos patikrinimas B. Reguliarus auditas C. Vidinės/tarnybinės patikros D. Nevyksta reguliavimo procedūros
8.	Incidento įtaka proceso reguliavimui	A. Skiriamos baudos B. Padidinamas auditorių dėmesys C. Gaunami nurodymai be baudžiamųjų sankcijų D. Niekas nevyksta	A. Skiriamos baudos B. Padidinamas auditorių dėmesys C. Gaunami nurodymai be baudžiamųjų sankcijų D. Niekas nevyksta
Reputacijos lygis			
9.	Įtaka įmonės reputacijai	A. Reputacija pažeminama tautiniu lygmeniu B. Reputacija pažeminama regioniniu lygmeniu C. Reputacija pažeminama internete D. Reputacija nepažeminama	A. Reputacija pažeminama tautiniu lygmeniu B. Reputacija pažeminama regioniniu lygmeniu C. Reputacija pažeminama internete D. Reputacija nepažeminama
Grėsmės arba pažeidžiamumo išnaudojimo asmenų potencialas			
10.	Kas turi prieigą prie IT infrastruktūros	A. Techninės priežiūros personalas (IT darbuotojai) B. Aptarnaujantis personalas (specialistai, operatoriai) C. Tretieji asmenys D. Nekvalifikuoti darbuotojai	A. Techninės priežiūros personalas (IT darbuotojai) B. Aptarnaujantis personalas (specialistai, operatoriai) C. Tretieji asmenys D. Nekvalifikuoti darbuotojai
11.	Kas atlieka duomenų operavimo funkciją	A. Techninės priežiūros personalas B. Kvalifikuoti vartotojai C. Nekvalifikuoti vartotojai D. Duomenimis nėra operuojama rankiniu būdu	A. Techninės priežiūros personalas B. Kvalifikuoti vartotojai C. Nekvalifikuoti vartotojai D. Duomenimis nėra operuojama rankiniu būdu
Taikomų prevencijos priemonių efektyvumas			
12.	Taikomos prevencijos priemonės	A. Apsaugos įranga nuo neteisėto įsibrovimo į įmonės tinklą B. Kenkėjiškų programų aptikimo programinė įranga C. Tinklo skirstymo priemonės D. VPN priemonės E. Virtualizavimo priemonių apsauga F. Neteisėto įsibrovimo į įmonės tinklą aptikimo įranga G. Apsaugos analizės priemonės	A. Apsaugos įranga nuo neteisėto įsibrovimo į įmonės tinklą B. Kenkėjiškų programų aptikimo programinė įranga C. Tinklo skirstymo priemonės D. VPN priemonės E. Virtualizavimo priemonių apsauga F. Neteisėto įsibrovimo į įmonės tinklą aptikimo įranga G. Apsaugos analizės priemonės

6. Ryšių su visuomene procesai			
Nr.	Klausimas	Ryšių su visuomene duomenų paviešinimas	Ryšių su visuomene duomenų praradimas
Informacinės sistemos kritiškumas			
1.	Interneto ryšio prieinamumas	A. Taip B. Ne	A. Taip B. Ne
2.	Duomenų perdavimo ryšys	A. Išorinis tinklas B. Vietinis tinklas	A. Išorinis tinklas B. Vietinis tinklas
3.	Naudojama kompiuterinės įrangos infrastruktūra	A. Fiziniai serveriai B. Virtualūs serveriai C. Personaliniai kompiuteriai D. Automatizuotos darbo vietos	A. Fiziniai serveriai B. Virtualūs serveriai C. Personaliniai kompiuteriai D. Automatizuotos darbo vietos
4.	Sistemos tipas	A. Uždaroji sistema, atliekanti apsaugos ir įvykių analizės funkcijas B. Tarnybinė stotis, kaupianti ir apdorojanti duomenys C. Palaikymo sistema, vizualizuojanti duomenis D. Atviroji sistema (tinklapis, informacinis žiniatinklis)	A. Uždaroji sistema, atliekanti apsaugos ir įvykių analizės funkcijas B. Tarnybinė stotis, kaupianti ir apdorojanti duomenys C. Palaikymo sistema, vizualizuojanti duomenis D. Atviroji sistema (tinklapis, informacinis žiniatinklis)
Procesų pažeidžiamumo lygis			
5.	IT infrastruktūros procesų funkcija	A. Užtikrina kelių procesų veiklą B. Užtikrina vieno proceso veiklą C. Užtikrina procesų palaikymą D. Neįtakoja procesų veiklos	A. Užtikrina kelių procesų veiklą B. Užtikrina vieno proceso veiklą C. Užtikrina procesų palaikymą D. Neįtakoja procesų veiklos
6.	IT infrastruktūros funkcijos sutrikimo įtaka procesams	A. Sustabdo kelių procesų veiklą B. Sustabdo vieno proceso veiklą C. Sulėtina procesų įgyvendinimą D. Neįtakoja procesų	A. Sustabdo kelių procesų veiklą B. Sustabdo vieno proceso veiklą C. Sulėtina procesų įgyvendinimą D. Neįtakoja procesų
Organizacijos veiklos reguliavimas			
7.	Procesas reguliuojamas	A. Atsitiktiniu metu vykdomas komisijos patikrinimas B. Reguliarus auditas C. Vidinės/tarnybinės patikros D. Nevyksta reguliavimo procedūros	A. Atsitiktiniu metu vykdomas komisijos patikrinimas B. Reguliarus auditas C. Vidinės/tarnybinės patikros D. Nevyksta reguliavimo procedūros
8.	Incidento įtaka proceso reguliavimui	A. Skiriamos baudos B. Padidinamas auditorių dėmesys C. Gaunami nurodymai be baudžiamųjų sankcijų D. Niekas nevyksta	A. Skiriamos baudos B. Padidinamas auditorių dėmesys C. Gaunami nurodymai be baudžiamųjų sankcijų D. Niekas nevyksta
Reputacijos lygis			
9.	Įtaka įmonės reputacijai	A. Reputacija pažeminama tautiniu lygmeniu B. Reputacija pažeminama regioniniu lygmeniu C. Reputacija pažeminama internete D. Reputacija nepažeminama	A. Reputacija pažeminama tautiniu lygmeniu B. Reputacija pažeminama regioniniu lygmeniu C. Reputacija pažeminama internete D. Reputacija nepažeminama
Grėsmės arba pažeidžiamumo išnaudojimo asmenų potencialas			
10.	Kas turi prieigą prie IT infrastruktūros	A. Techninės priežiūros personalas (IT darbuotojai) B. Aptarnaujantis personalas (specialistai, operatoriai) C. Tretieji asmenys D. Nekvalifikuoti darbuotojai	A. Techninės priežiūros personalas (IT darbuotojai) B. Aptarnaujantis personalas (specialistai, operatoriai) C. Tretieji asmenys D. Nekvalifikuoti darbuotojai
11.	Kas atlieka duomenų operavimo funkciją	A. Techninės priežiūros personalas B. Kvalifikuoti vartotojai C. Nekvalifikuoti vartotojai D. Duomenimis nėra operuojama rankiniu būdu	A. Techninės priežiūros personalas B. Kvalifikuoti vartotojai C. Nekvalifikuoti vartotojai D. Duomenimis nėra operuojama rankiniu būdu
Taikomų prevencijos priemonių efektyvumas			
12.	Taikomos prevencijos priemonės	A. Apsaugos įranga nuo neteisėto įsibrovimo į įmonės tinklą B. Kenkėjiškų programų aptikimo programinė įranga C. Tinklo skirstymo priemonės D. VPN priemonės E. Virtualizavimo priemonių apsauga F. Neteisėto įsibrovimo į įmonės tinklą aptikimo įranga G. Apsaugos analizės priemonės	A. Apsaugos įranga nuo neteisėto įsibrovimo į įmonės tinklą B. Kenkėjiškų programų aptikimo programinė įranga C. Tinklo skirstymo priemonės D. VPN priemonės E. Virtualizavimo priemonių apsauga F. Neteisėto įsibrovimo į įmonės tinklą aptikimo įranga G. Apsaugos analizės priemonės

7 PRIEDAS. APKLAUSOS VERTINIMO METODIKA

1 klausimas	2 klausimas	3 klausimas	4 klausimas	5 klausimas	6 klausimas
A = 1 balas B = 0 balų	A = 1 balas B = 0 balų	Galimi keli atsakymai po 0,25 balo (rezultatai sumuojami)	Galimi keli atsakymai po 0,25 balo (rezultatai sumuojami)	A = 2 balai B = 1,5 balo C = 1 balas D = 0,5 balo	A = 2 balai B = 1,5 balo C = 1 balas D = 0,5 balo
1 – 4 klausimų rezultatai sumuojami. Didžiausias rezultatas – 4 balai. 1 balas atitinka 0,25 balo galimo nuostolių lygio ir grėsmės realizavimo tikimybės kriterijų lygio. 5 – 6 klausimų rezultatai sumuojami. Didžiausias rezultatas – 4 balai. 1 balas atitinka 0,25 balo galimo nuostolių lygio ir grėsmės realizavimo tikimybės kriterijų lygio.					
7 klausimas	8 klausimas	9 klausimas	10 klausimas	11 klausimas	12 klausimas
A = 2 balai B = 1,5 balo C = 1 balas D = 0,5 balo	A = 2 balai B = 1,5 balo C = 1 balas D = 0,5 balo	A = 4 balai B = 3 balai C = 2 balai D = 1 balas	A = 2 balai B = 1,5 balo C = 1 balas D = 0,5 balo	A = 2 balai B = 1,5 balo C = 1 balas D = 0,5 balo	Galimi keli atsakymai A – F po 0,5 balo G = 1 balas (rezultatai sumuojami)
7 – 8 klausimų rezultatai sumuojami. Didžiausias rezultatas – 4 balai. 1 balas atitinka 0,25 balo galimo nuostolių lygio ir grėsmės realizavimo tikimybės kriterijų lygio. 9 klausimo didžiausias rezultatas – 4 balai. 1 balas atitinka 0,25 balo galimo nuostolių lygio ir grėsmės realizavimo tikimybės kriterijų lygio. 10 – 11 klausimo rezultatai sumuojami. Didžiausias rezultatas – 4 balai. 1 balas atitinka 0,25 balo galimo nuostolių lygio ir grėsmės realizavimo tikimybės kriterijų lygio. 12 klausimo didžiausias rezultatas – 4 balai. 1 balas atitinka 0,25 balo galimo nuostolių lygio ir grėsmės realizavimo tikimybės kriterijų lygio.					



VILNIAUS GEDIMINO
TECHNIKOS UNIVERSITETAS
FUNDAMENTINIŲ MOKSLŲ FAKULTETAS
INFORMACINIŲ SISTEMŲ KATEDRA

PAŽYMĖJIMAS

Nr. 19-0424-10

Patvirtinantis, kad

Roman Jevsejev

dalyvavo 22-osios Lietuvos jaunųjų mokslininkų konferencijos

„**MOKSLAS – LIETUVOS ATEITIS**“ teminėje konferencijoje

INFORMACINIŲ TECHNOLOGIJŲ SAUGA IR INFORMACINĖS SISTEMOS,

parengė ir pristatė pranešimą

„**IT rizikos valdymo metodo patobulinimas**“.

Mokslo komiteto pirmininkas

Organizacinio komiteto pirmininkas

prof. dr. Dalius Mažeika

doc. dr. Nikolaj Goranin

Vilnius, 2019