www.mruni.eu

Lina LELEŠIENĖ

Daktaro disertacija

KIBERNETINIO SAUGUMO VALDYMO MODELIO E. SVEIKATOS SISTEMOS TOBULINIMUI VERTINIMAS

SOCIALINIAI MOKSLAI,
VADYBA (S 003)
VILNIUS, 2026

Mykolo Romerio universitetas

MYKOLO ROMERIO UNIVERSITETAS

Lina Lelešienė

KIBERNETINIO SAUGUMO VALDYMO MODELIO E. SVEIKATOS SISTEMOS TOBULINIMUI VERTINIMAS

Mokslo daktaro disertacija
Socialiniai mokslai, vadyba (S 003)

Vilnius, 2026

Mokslo daktaro disertacija rengta 2020-2026 metais Mykolo Romerio universitete pagal Vytauto Didžiojo universitetui su Klaipėdos universitetu, Mykolo Romerio universitetu ir Vilniaus universitetu Lietuvos Respublikos švietimo, mokslo ir sporto ministro 2019 m. vasario 22 d. įsakymu Nr. V-160 suteiktą doktorantūros teisę.

Mokslinis vadovas:
prof. dr. Tadas Limba (Mykolo Romerio universitetas, socialiniai mokslai, vadyba, S 003).

Mokslo daktaro disertacija ginama Vytauto Didžiojo universiteto, Klaipėdos universiteto, Mykolo Romerio universiteto ir Vilniaus universiteto Šiaulių akademijos vadybos mokslo krypties taryboje:

Pirmininkas:
prof. dr. Andrius Stasiukynas (Mykolo Romerio universitetas, socialiniai mokslai, vadyba, S 003).

Nariai:
prof. dr. Vida Davidavičienė (Vilniaus Gedimino technikos universitetas, socialiniai mokslai, vadyba, S 003);
prof. dr. Iveta Reinholde (Latvijos universitetas, Latvijos Respublika, socialiniai mokslai, politikos mokslai, S 002);
prof. dr. Rimantas Stašys (Klaipėdos universitetas, socialiniai mokslai, vadyba, S 003);
prof. dr. Jolita Vveinhardt (Vytauto Didžiojo universitetas, socialiniai mokslai, vadyba, S 003).

Mokslo daktaro disertacija bus ginama viešame Vadybos mokslo krypties tarybos posėdyje 2026 m. lapkričio 10 d. 10 val. Mykolo Romerio universitete, I-414 auditorijoje.
Adresas: Ateities g. 20, 08303 Vilnius.

© Mykolo Romerio universitetas, 2026

TURINYS

PAVEIKSLŲ SĄRAŠAS 6

LENTELIŲ SĄRAŠAS 7

PRIEDŲ SĄRAŠAS 9

PAGRINDINĖS SĄVOKOS 10

SANTRUMPOS 12

ĮVADAS 14

1. KIBERNETINIO SAUGUMO VALDYMO TEORINIAI ASPEKTAI 21
1.1. Kibernetinio saugumo samprata ir reikšmė 21
1.1.1. Kibernetinio saugumo sąvokos raida 22
1.1.2. Kibernetinio saugumo pagrindiniai principai ir tikslai 23
1.1.3. Kibernetinio saugumo svarba skaitmenizuotoje visuomenėje 25
1.2. Kibernetinio saugumo grėsmės ir rizikos 26
1.2.1. Kibernetinių incidentų klasifikacija 28
1.2.2. Rizikų veiksniai e. sveikatos srityje 30
1.2.3. Kibernetiniai incidentai ir jų pasekmės 32
1.3. Informacijos saugumo valdymo sistemos 34
1.3.1. ISO/IEC 27001, 27005 ir susiję standartai 35
1.3.2. TIS2 direktyva ir jos įgyvendinimas 37
1.3.3. Kibernetinio saugumo brandos modeliai 40
1.4. Kibernetinio saugumo valdymas sveikatos sektoriuje 42
1.4.1. E. sveikatos sistemos struktūra ir veikimo principai 45
1.4.2. Informacinių sistemų integracija ir sąveika 53
1.4.3. Duomenų apsauga ir konfidencialumas sveikatos sektoriuje 56
1.4.4. E. sveikatos sistemos kibernetinis atsparumas ir jo operaciniai rodikliai.. 57

2. KIBERNETINIO SAUGUMO VALDYMO MODELIO E. SVEIKATOS SISTEMOS TOBULINIMUI STRUKTŪROS KŪRIMAS IR TYRIMO METODOLOGIJA 65
2.1. Kibernetinio saugumo valdymo modelių analizė 65
2.1.1. Teorinių kibernetinio saugumo valdymo modelių analizė 66
2.1.2. Praktiniai kibernetinio saugumo valdymo modeliai taikomi sveikatos sektoriuje 67

2.1.3. Tarpinstituciniai kibernetinio saugumo valdymo modeliai ir jų efektyvumo vertinimas 69
2.2. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui kūrimo principai ir reikalavimai 72
2.2.1. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui funkciniai ir nefunkciniai reikalavimai 74
2.2.2. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui pritaikomumo principai 80
2.2.3. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui struktūros komponentų identifikavimas 82
2.3. Prielaidos kibernetinio saugumo valdymo modeliui e. sveikatos sistemos tobulinimui kurti 84
2.3.1. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui valdymo lygiai ir hierarchija 85
2.3.2. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui informacijos srautų saugumas 87
2.3.3. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui atsakomybės pasiskirstymas 90
2.3.4. Koncepcinio kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui kūrimas 91
2.4. Tyrimo metodologija 97
2.4.1. Tyrimo tikslas, uždaviniai ir tiriamieji klausimai 99
2.4.2. Tyrimo dizainas 101
2.4.3. Tyrimo imtis, ekspertų atranka ir atrankos kriterijai 102
2.4.4. Duomenų rinkimo priemonės 106
2.4.5. Duomenų analizės metodai 107

3. EMPIRINIO TYRIMO REZULTATAI IR KIBERNETINIO SAUGUMO VALDYMO MODELIO E. SVEIKATOS SISTEMOS TOBULINIMUI TIKSLINIMAS 110
3.1. Ekspertų nuomonės vertinimo tyrimo analizės struktūra 110
3.1.1. Ekspertų sociodemografinis profilis 111
3.1.2. Kibernetinio saugumo valdymo lygio vertinimas sveikatos įstaigose ekspertų požiūriu 113
3.1.3. Kibernetinio saugumo spragų identifikavimas e. sveikatos sistemoje ekspertų požiūriu 114
3.1.4. Rizikų ir incidentų valdymo praktikos vertinimas ekspertų požiūriu 117
3.2. Teminė ekspertinė interviu analizė 119

3.2.1. Strateginio ir organizacinio valdymo problematika 122
3.2.2. Technologinio saugumo ir procesų brandos vertinimas 124
3.2.3. Teisinio reglamentavimo ir praktinio įgyvendinimo atotrūkiai 127
3.3. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui tikslinimas remiantis ekspertinio tyrimo rezultatais 129
3.3.1. Kritinių kibernetinio saugumo valdymo sričių identifikavimas 130
3.3.2. Patikslintas kibernetinio saugumo valdymo modelis e. sveikatos sistemos tobulinimui: struktūrinių ir funkcinių siūlymų integracija 133
3.3.3. Patikslinto kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui adaptavimas praktiniam taikymui e. sveikatos sistemoje 142
3.3.4. E. sveikatos kibernetinio saugumo valdymo brandos vertinimo metodika, grindžiama siūlomu modeliu 145
3.4. Patikslinto kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui ekspertinis vertinimas 148
3.4.1. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui tinkamumo ir taikymo galimybių vertinimas 148
3.4.2. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui stiprybės, ribotumai ir strateginės kryptys 153
IŠVADOS 159
REKOMENDACIJOS 163
LITERATŪRA 166
PRIEDAI 184
SANTRAUKA 219
MOKSLINIŲ PUBLIKACIJŲ SĄRAŠAS 242
SUMMARY 245

PAVEIKSLŲ SĄRAŠAS

1 pav. Disertacinio darbo struktūros loginė schema 20
2 pav. Lietuvos e. sveikatos sistemos raida ir kibernetinio saugumo reikšmė 2005–2026 m. 48
3 pav. E. sveikatos sistemos kibernetinio atsparumo operacinės dimensijos ir rodikliai 62
4 pav. E. sveikatos sistemos kibernetinio atsparumo operacionalizavimo schema 79
5 pav. Koncepcinis kibernetinio saugumo valdymo modelis e. sveikatos sistemos tobulinimui 93
6 pav. Dizaino mokslo tyrimų metodologija 98
7 pav. Ekspertų skaičiaus įtaka vertinimo patikimumui 103
8 pav. Problemos, išryškėjusios ekspertų interviu metu 131
9 pav. Patikslintas kibernetinio saugumo valdymo modelis e. sveikatos sistemos tobulinimui 134
10 pav. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui adaptavimo vykdymas etapais 144
11 pav. E. sveikatos kibernetinio saugumo valdymo brandos vertinimo skalė ... 146
12 pav. Pagrindinės kibernetinio saugumo modelio e. sveikatos sistemos tobulinimui plėtros kryptys 156

LENTELIŲ SĄRAŠAS

1 lentelė. Kibernetinių incidentų klasifikavimo požiūrių palyginimas 29

2 lentelė. Kibernetinių rizikų veiksniai e. sveikatos sistemose ir jų poveikis 31

3 lentelė. Kibernetinių incidentų tipai e. sveikatos sistemose, jų apibrėžimai ir pasekmės 33

4 lentelė. TIS2 (*angl. NIS2*) direktyvos reikalavimų suvedimas į kibernetinio saugumo valdymo modelio dimensijas 39

5 lentelė. Kibernetinio saugumo valdymo modelio teorinių ir normatyvinių šaltinių reikšmė bei ribotumai e. sveikatos sistemos kontekste 42

6 lentelė. E. sveikatos sistemos struktūriniai komponentai ir jų veikimo logika kibernetinio saugumo valdymo požiūriu 52

7 lentelė. Informacinių sistemų sąveikos tipai e. sveikatos sistemose, rizikos ir brandos indikatoriai 55

8 lentelė. Teorinių kibernetinio saugumo valdymo modelių palyginamoji analizė 67

9 lentelė. Praktinių kibernetinio saugumo valdymo modelių taikymas e. sveikatos sektoriuje 69

10 lentelė. Tarpinstitucinių kibernetinio saugumo valdymo modelių tipai ir jų efektyvumo vertinimo kriterijai 70

11 lentelė. Funkcinių ir nefunkcinių kibernetinio saugumo valdymo reikalavimų sąsajos su empiriniais vertinimo indikatoriais e. sveikatos sistemos kontekste 76

12 lentelė. Informacijos srautų saugumo dimensijos e. sveikatos sistemose ir jų empiriniai indikatoriai 89

13 lentelė. Ekspertų ir interviu informacija 106

14 lentelė. Respondentų sociodemografinės ir profesinės charakteristikos 112

15 lentelė. Teminė ekspertinių interviu analizė 120

16 lentelė. Vertinimo kriterijai 151

17 lentelė. Ekspertų suteikti rangai 151

18 lentelė. Rangų sumų nuokrypių skaičiavimas 152

19 lentelė. Patikslinto kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui stiprybių, ribotumų ir strateginių krypčių sintezė 155

20 lentelė. Tiriamųjų klausimų (TK1–TK4) analizės rezultatų apibendrinimas . 157

21 lentelė. TK1 tiriamojo klausimo teminės analizės kategorijos 188

22 lentelė. TK1 tiriamojo klausimo teminių kategorijų pasireiškimas ekspertų interviu duomenyse 189

23 lentelė. TK1 tiriamojo klausimo analitinių kategorijų ekspertinis rangavimas 190
24 lentelė. TK1 rangų sumų nuokrypių skaičiavimas 191
25 lentelė. TK2 tiriamojo klausimo teminės analizės kategorijos 194
26 lentelė. TK2 tiriamojo klausimo teminių kategorijų pasireiškimas ekspertų interviu duomenyse 195
27 lentelė. TK2 tiriamojo klausimo analitinių kategorijų ekspertinis rangavimas 196
28 lentelė. TK2 tiriamojo klausimo analitinių kategorijų rangų sumų nuokrypių skaičiavimas 197
29 lentelė. TK3 tiriamojo klausimo teminės analizės kategorijos 200
30 lentelė. TK3 tiriamojo klausimo teminių kategorijų pasireiškimas ekspertų interviu duomenyse 201
31 lentelė. TK3 tiriamojo klausimo analitinių kategorijų ekspertinis rangavimas 202
32 lentelė. TK3 tiriamojo klausimo analitinių kategorijų rangų sumų nuokrypių skaičiavimas 203
33 lentelė. TK4 tiriamojo klausimo teminės analizės kategorijos 206
34 lentelė. TK4 tiriamojo klausimo teminių kategorijų pasireiškimas ekspertų interviu duomenyse 207
35 lentelė. TK4 tiriamojo klausimo analitinių kategorijų ekspertinis rangavimas 208
36 lentelė. TK4 tiriamojo klausimo analitinių kategorijų rangų sumų nuokrypių skaičiavimas 209
37 lentelė. Kibernetinio saugumo valdymo brandos vertinimo matrica 212
38 lentelė. Bendro brandos indekso interpretavimas 216
39 lentelė. Operacinių rodiklių sąrašas 216

PRIEDŲ SĄRAŠAS

1 priedas. Ekspertinio pusiau struktūrizuoto interviu klausimynas 184
2 priedas. TK1 tiriamojo klausimo kokybinės analizės rezultatai 188
3 priedas. TK2 tiriamojo klausimo kokybinės analizės rezultatai 193
4 priedas. TK3 tiriamojo klausimo kokybinės analizės rezultatai 199
5 priedas. TK4 tiriamojo klausimo kokybinės analizės rezultatai 205
6 priedas. E. sveikatos kibernetinio saugumo valdymo brandos vertinimo matrica, grindžiama siūlomu modeliu 211

PAGRINDINĖS SĄVOKOS

Atsparumas kibernetinėms grėsmėms / kibernetinis atsparumas	e. sveikatos sistemos gebėjimas numatyti kibernetines grėsmes, pasirengti incidentams, atlaikyti jų poveikį, išlaikyti kritinių paslaugų teikimą, atkurti sutrikusias funkcijas ir prisitaikyti prie pasikeitusios rizikos aplinkos (Linkov ir kt., 2019; NIST, 2020).
Asmens duomenys	bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius (Bendrasis asmens duomenų apsaugos reglamentas, 2016).
E. sveikata	trijų sričių integracija: sveikatos apsaugos, medicininės informacijos ir organizacijų, kurios teikia sveikatos priežiūros e. paslaugas (Eysenbach, 2001).
Socio-techninė e. sveikatos sistema	sistema, kurioje technologiniai sprendimai yra neatsiejami nuo organizacinių ir socialinių veiksnių (Hochwarter, 2021).
E. receptas	integruota e. sveikatos sistemos funkcinė posistemė, leidžianti saugiai generuoti, perduoti ir administruoti medicininius receptus skaitmeninėje aplinkoje, užtikrinant duomenų vientisumą, prieinamumą ir sąveikumą tarp sveikatos priežiūros subjektų.
Kibernetinis saugumas	visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2024).

Kibernetinio saugumo valdymo modelis e. sveikatos sistemos tobulinimui	dinamiška struktūra, apibrėžianti kibernetinio saugumo valdymo principus, valdymo lygmenis, funkcines dimensijas ir jų tarpusavio sąveikas, skirta sistemingam kibernetinio saugumo užtikrinimui ir tobulinimui e. sveikatos sistemoje.
Kibernetinis incidentas	įvykis, dėl kurio kyla pavojus saugomų, perduodamų arba tvarkomų duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas, prieinamumui, autentiškumui, vientisumui arba konfidencialumui (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2024).
Kibernetinių incidentų valdymas	procedūros, kurių tikslas – aptikti, analizuoti kibernetinius incidentus ir reaguoti į juos, taip pat atkurti įprastinę ryšių ir informacinių sistemų veiklą (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2024).
Modelis	objektas, struktūra arba abstrakti reprezentacija, skirta parodyti, kaip tam tikras reiškinys, sistema ar procesas atrodo, veikia arba gali būti suprantamas; taip pat gali būti naudojamas prognozuoti galimus rezultatus remiantis tam tikromis prielaidomis (Cambridge Dictionary, n.d.).

SANTRUMPOS

BDAR	Bendrasis duomenų apsaugos reglamentas
COBIT	(angl. *Control Objectives for Information and Related Technologies*) – informacinių technologijų valdymo ir valdymo kontrolės sistema, skirta užtikrinti informacinių technologijų procesų atitiktį organizacijos strateginiams tikslams.
CSIRT	(angl. *Computer Security Incident Response Team*) – kompiuterinių saugumo incidentų reagavimo komanda.
E. sveikata	elektroninė sveikata
ENISA	(angl. *European Union Agency for Cybersecurity*) – Europos Sąjungos kibernetinio saugumo agentūra.
ES	Europos Sąjunga
IAM	(angl. *Identity and Access Management*) – tapatybės ir prieigos valdymas, apimantis naudotojų tapatybės nustatymo, autentifikavimo ir autorizavimo procesus.
IoMT	(angl. *Internet of Medical Things*) – medicininių įrenginių, prijungtų prie tinklų ir naudojamų sveikatos duomenų rinkimui, perdavimui ir apdorojimui, visuma.
ISMS	(angl. *Information Security Management System*) – informacijos saugumo valdymo sistema, apimanti politikų, procedūrų, procesų ir kontrolės priemonių visumą, skirtą informacijos saugumui užtikrinti.
TIS2 (NIS2)	Europos Parlamento ir Tarybos direktyva (ES) 2022/2555
PDCA	(angl. *Plan Do Check Act*) – nuolatinio tobulinimo ciklas, naudojamas valdymo sistemose, įskaitant kibernetinio saugumo ir kokybės valdymą.

SABSA	(angl. *Sherwood Applied Business Security Architecture*) – rizikomis grindžiama saugumo architektūros metodologija, skirta saugumo sprendimų derinimui su organizacijos verslo tikslais.
SIEM	(angl. *Security Information and Event Management*) – saugumo informacijos ir įvykių valdymo sistema, skirta saugumo įvykių rinkimui, koreliavimui ir analizei.
TIS	Tinklų ir informacinių sistemų saugumas

ĮVADAS

Temos aktualumas. E. sveikatos sistemos plėtra iš esmės keičia sveikatos priežiūros paslaugų organizavimą ir duomenų valdymą. Vis daugiau sveikatos priežiūros procesų vyksta skaitmeninėje aplinkoje – nuo elektroninių sveikatos įrašų ir e. recepto iki pacientų registracijos, medicininių dokumentų mainų bei duomenų perdavimo tarp sveikatos priežiūros įstaigų. Tokie sprendimai padeda greičiau keistis informacija, efektyviau organizuoti paslaugas ir sudaro patogesnes sąlygas tiek pacientams, tiek sveikatos priežiūros specialistams.

Kartu didėjanti skaitmenizacija sukuria ir naujų kibernetinio saugumo iššūkių. E. sveikatos sistemoje tvarkomi itin jautrūs asmens sveikatos duomenys, o skirtingų informacinių sistemų tarpusavio sąveika reiškia, kad saugumo pažeidimas vienoje grandyje gali paveikti ir kitus sistemos dalyvius. Duomenų nutekinimas, neautorizuota prieiga, e. recepto, pacientų portalo ar medicininių dokumentų mainų sutrikimai gali turėti pasekmių ne tik duomenų apsaugai, bet ir paslaugų tęstinumui bei pacientų pasitikėjimui. Todėl e. sveikatos kibernetinis saugumas turi būti suprantamas ne vien kaip techninių apsaugos priemonių taikymas, bet kaip nuoseklus valdymo procesas, apimantis rizikų vertinimą, atsakomybių paskirstymą, incidentų valdymą, duomenų apsaugą ir nuolatinį sistemos tobulinimą.

Pastaraisiais metais sveikatos sektorius vis dažniau įvardijamas kaip vienas iš pažeidžiamiausių kibernetinių atakų taikinių, nes jame susikerta jautrių duomenų apsauga, kritinių paslaugų tęstinumas ir riboti organizaciniai ištekliai. Tai rodo, kad vien pavienėmis techninėmis priemonėmis grįstas saugumo valdymas nėra pakankamas. Sveikatos priežiūros įstaigos tampa ypač patraukliu taikiniu dėl jų valdomų ypač jautrių duomenų, kritinės infrastruktūros statuso ir dažnai ribotų išteklių pažangioms saugumo priemonėms diegti. Išpirkos reikalaujančios (angl. *ransomware*) atakos, asmens duomenų saugumo pažeidimai, paslaugų trikdymai, neautorizuotos prieigos prie e. sveikatos informacinių sistemų ar tinkle veikiančių medicininių prietaisų atvejai kelia riziką ne tik asmens duomenų apsaugai, bet ir sveikatos paslaugų tęstinumui, o tai gali tiesiogiai paveikti pacientų saugumą. Dėl šios priežasties šiame darbe kibernetinio saugumo valdymas nagrinėjamas ne kaip pavienių techninių priemonių rinkinys, o kaip nuoseklus valdymo procesas, pritaikytas e. sveikatos sistemos struktūrai ir jos veikimo specifikai. Reglamentavimo lygmeniu kibernetinio saugumo svarba nuosekliai didėja, o teisės aktai (tokie dokumentai kaip TIS2 direktyva, BDAR, ISO/IEC 27001, ISO/IEC 27005:2018, ISO/IEC 27035-1:2023, ISO/IEC 27701:2019 ir ISO/IEC 27032:2023) įtvirtina griežtesnius informacijos saugumo ir rizikų valdymo reikalavimus, akcentuoja poreikį sistemingam informacijos saugumo valdymui, rizikos vertinimo procesų integracijai ir nuolatiniam organizacijų saugumo brandos didinimui. Vis dėlto praktikoje sveikatos sektoriaus organizacijos dažnai susiduria su iššūkiais perkeliant šiuos standartus į realius vadybinius sprendimus. Dėl to šiame darbe pagrindžiamas poreikis formuoti tokį kibernetinio saugumo valdymo modelį, kuris sujungtų tarptautinių standartų nuostatas, nacionalinį reguliavimą ir e. sveikatos sistemos organizacinę bei technologinę specifiką.

Temos aktualumą stiprina ir organizaciniai veiksniai. Sveikatos priežiūros įstaigų gebėjimas valdyti kibernetinį saugumą priklauso ne tik nuo technologijų, bet ir nuo darbuotojų kompetencijų, atsakomybių paskirstymo, vidinių procedūrų ir vadovybės įsitraukimo. Empiriniai tyrimai rodo, kad kibernetinio saugumo kultūra, darbuotojų žinios ir įgūdžiai, aiškiai apibrėžti valdymo procesai bei organizacinės struktūros veiksmingumas lemia, kaip efektyviai sveikatos sektoriaus institucijos gali įgyvendinti saugumo priemones ir reaguoti į kylančias grėsmes. Tačiau sveikatos sektoriuje vis dar trūksta empirinių modelių, leidžiančių įvertinti ir palyginti kibernetinio saugumo valdymo brandą skirtinguose e. sveikatos sistemos lygmenyse. Todėl mokslinis indėlis, kuriant ir vertinant kibernetinio saugumo valdymo modelį, gali turėti reikšmingą praktinę vertę, didinant sprendimų priėmimo efektyvumą, išteklių paskirstymo racionalumą ir organizacijų atsparumą kibernetinėms grėsmėms.

Šioje disertacijoje e. sveikatos sistemos kibernetinio saugumo valdymas traktuojamas kaip mokslinė ir praktinė problema, kylanti iš e. sveikatos infrastruktūros kompleksiškumo, didėjančių kibernetinių rizikų ir poreikio valdymo sprendimus susieti su konkrečia e. sveikatos sistemos struktūra.

Nors informacijos saugumo valdymas plačiai nagrinėjamas ekonomikos ir vadybos srityse, esamų žinių nepakanka kuriant kibernetinio saugumo valdymo modelius, pritaikomus e. sveikatos sistemoms. Mokslininkai pabrėžia, kad kritinės infrastruktūros apsauga reikalauja kompleksinio požiūrio, o e. sveikatos sistema yra viena svarbiausių sveikatos sektoriaus inovacijų, kuri pasižymi dideliu duomenų jautrumu ir procesų sudėtingumu. Nors jos ekonominė, socialinė ir organizacinė nauda yra akivaizdi, sukurti vertės vertinimą leidžiančius metodus vis dar sudėtinga. Praktikoje taikomi įvairūs vertinimo modeliai padeda matuoti efektyvumą ir optimizuoti procesus, tačiau jų taikymas kinta priklausomai nuo sistemos tikslų, suinteresuotųjų šalių ir konteksto. Kadangi e. sveikatos paslaugos tiesiogiai susijusios su žmogaus sveikata ir jautriai vertinamos vartotojų, būtina turėti specialiai šiai sričiai pritaikytą kibernetinio saugumo valdymo modelį. Nepaisant šios srities aktualumo, kibernetinio saugumo valdymas e. sveikatos kontekste tarptautiniu mastu išlieka nepakankamai ištirtas.

Disertacijoje siekiama suformuoti kibernetinio saugumo valdymo modelį, kuris galėtų būti veiksmingai taikomas e. sveikatos sistemos kūrimo ir administravimo procesuose. Vienas iš ryškiausių iššūkių, su kuriais susiduria e. sveikatos infrastruktūra, yra nepakankamai užtikrinamas informacinių sistemų saugumas. Šiame darbe daroma prielaida, kad šioje disertacijoje kuriamas kibernetinio saugumo valdymo modelis gali sudaryti prielaidas nuoseklesnei ir spartesnei e. sveikatos sprendimų plėtrai. Šiuolaikinė technologinė raida lemia vis intensyvesnį jautrių duomenų perkėlimą į skaitmeninę aplinką, todėl kibernetinio saugumo problematika tampa vis aktualesnė tiek organizacijoms, tiek individualiems vartotojams. Didėjant priklausomybei nuo skaitmeninių paslaugų, auga ir pažeidžiamumas, o tai skatina tyrėjų ir visuomenės domėjimąsi šia sritimi. Norint veiksmingai valdyti kylančias rizikas, būtina kryptingai identifikuoti galimas grėsmes, vertinti jų poveikį ir numatyti prevencines priemones, užtikrinančias savalaikį jų suvaldymą.

Apibendrinus disertacijoje nagrinėtą mokslinę literatūrą, matyti keli probleminiai

aspektai, kylantys modeliuojant kibernetinio saugumo valdymo modelį e. sveikatos sistemų plėtros procese. Pirmiausia išryškėja sunkumai pasirenkant ir pritaikant tinkamiausius kibernetinio saugumo modelius, kurie galėtų būti taikomi kuriant ir tobulinant e. sveikatos infrastruktūrą. Taip pat pabrėžiama būtinybė aiškiai apibrėžti norimą rezultatą, nes tai lemia tinkamo valdymo modelio pasirinkimą ir jo pritaikymo logiką. Galiausiai, literatūroje akcentuojamas poreikis kurti vertinimo kriterijus, leidžiančius analizuoti ne atskirus sistemos elementus, bet visą e. sveikatos ekosistemą kaip vieningą darinį, taip sudarant galimybę integruoti skirtingus rodiklius į vientisą ir nuoseklų vertinimo pagrindą.

Taigi šioje disertacijoje kibernetinio saugumo valdymo modeliavimas analizuojamas kaip būdas sistemiškai susieti e. sveikatos infrastruktūros plėtrą, rizikų valdymą, incidentų valdymą, duomenų apsaugą ir atsparumo didinimo prielaidas.

Mokslinė problema – koks turi būti kibernetinio saugumo valdymo modelis, užtikrinantis veiksmingą e. sveikatos sistemos tobulinimą ir leidžiantis sumažinti kibernetinių grėsmių bei informacinių sistemų pažeidžiamumų rizikas?

Mokslinio tyrimo objektas – kibernetinio saugumo valdymo modelio vertinimas e. sveikatos sistemos kontekste.

Mokslinio tyrimo tikslas – parengti kibernetinio saugumo valdymo modelį e. sveikatos sistemos tobulinimui, sudarant prielaidas e. sveikatos sistemos atsparumui kibernetinėms grėsmėms didinti.

Tyrimo uždaviniai:

1. Išanalizuoti kibernetinio saugumo valdymo teorinius aspektus, principus ir esamus modelius, kibernetinio saugumo valdymo ypatumus e. sveikatos IS integracijos, duomenų apsaugos ir kibernetinio atsparumo kontekste.
2. Atlikti sisteminę e. sveikatos sistemų kibernetinių incidentų bei atakų analizę.
3. Parengti koncepcinį kibernetinio saugumo valdymo modelį, orientuotą į e. sveikatos sistemos projektavimo, diegimo, administravimo ir tobulinimo etapus.
4. Remiantis empirinio tyrimo ekspertų identifikuotomis problemomis ir gautais rezultatais, patikslinti sukurtą kibernetinio saugumo valdymo modelį e. sveikatos sistemos tobulinimui.
5. Ekspertiniu požiūriu įvertinti sukurto kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui tinkamumą, praktinį pritaikomumą, atitikimą sveikatos sektoriaus organizacijų praktikai ir galimus taikymo ribotumus.
6. Parengti rekomendacijas dėl patikslinto kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimo taikymo ir integravimo į e. sveikatos sistemos gerinimo procesus.

Mokslinio tyrimo metodai. Disertacijoje taikoma mokslinės literatūros, tarptautinių standartų ir teisės aktų lyginamoji analizė, siekiant identifikuoti kibernetinio saugumo valdymo principų, modelių ir metodikų taikymo kryptis, jų sąsajas bei skirtumus e. sveikatos sistemos kontekste. Teorinių šaltinių sisteminimas ir apibendrinimas

leidžia išryškinti pagrindinius kibernetinių incidentų kilmės veiksnius, e. sveikatos infrastruktūros pažeidžiamumus, taip pat suformuoti pradinį konceptualų kibernetinio saugumo valdymo modelį, orientuotą į e. sveikatos sistemos projektavimo, įgyvendinimo, administravimo ir tobulinimo procesus. Kai kurių mokslinių šaltinių ir citatų vertimui naudoti Europos Komisijos dirbtinio intelekto kalbos įrankiai.

Empirinėje tyrimo dalyje taikomas kokybinis tyrimo metodas – pusiau struktūruoti ekspertiniai interviu, kurių metu apklausiami kibernetinio saugumo valdymo, e. sveikatos sistemų administravimo, strateginio planavimo ir technologinių sprendimų diegimo srityse dirbantys specialistai. Ekspertų įžvalgos naudojamos pradinio modelio elementams tikslinti, įvertinti jų praktinį aktualumą, identifikuoti sistemines spragas ir suformuluoti modelio patobulinimus, atspindinčius realias e. sveikatos sistemos valdymo sąlygas.

Papildomai taikoma dokumentų analizė, leidžianti vertinti ekspertų pateiktas įžvalgas su normatyviniu reguliavimu, gairėmis, strateginiais dokumentais ir (kai aktualu) organizaciniais vidaus dokumentais. Interviu duomenys analizuojami taikant teminę analizę (angl. *thematic analysis*), sistemingai identifikuojant pasikartojančias temas, problemines sritis ir jų ryšius su modelio struktūriniais lygmenimis bei funkcinėmis dimensijomis. Remiantis teorinės analizės ir empirinio tyrimo rezultatais, atliekamas kibernetinio saugumo valdymo modelio koregavimas ir patobulinimas, o darbo pabaigoje formuluojamos apibendrintos mokslinės ir praktinės išvados bei rekomendacijos dėl modelio taikymo e. sveikatos sistemos tobulinimo procesuose.

Disertacijos ginamieji teiginiai:

1. E. sveikatos kibernetinio saugumo valdymo veiksmingumas priklauso nuo jo integravimo į bendrą organizacijos valdymą, vadovybės įsitraukimo ir aiškaus atsakomybių paskirstymo.
2. Kibernetinio saugumo valdymo fragmentiškumą mažina nuosekli strateginio, taktinio, operacinio ir technologinio valdymo lygmenų sąveika.
3. Patikslintas kibernetinio saugumo valdymo modelis sudaro metodinį pagrindą valdymo spragoms nustatyti ir prioritetinėms tobulinimo kryptims pagrįsti.

Darbo naujumas ir praktinis reikšmingumas. Kibernetinio saugumo valdymas e. sveikatos sistemos kontekste yra tarpdisciplinė sritis, kurioje susikerta informacinių technologijų, vadybos, teisės, viešojo administravimo ir sveikatos mokslų problematika. Nors pasaulyje atliekama nemažai tyrimų, nagrinėjančių kibernetinio saugumo klausimus, dauguma jų analizuoja šį reiškinį tik vienos mokslo krypties rėmuose, neatsižvelgdami į platesnį organizacinių, procesinių ir reguliacinių veiksnių kontekstą. Dėl šios priežasties kibernetinis saugumas dažnai traktuojamas fragmentiškai – kaip technologinis iššūkis arba kaip teisinės atitikties problema, nors veiksmingas saugumo užtikrinimas reikalauja integruoto, kelių mokslo sričių žiniomis grindžiamo požiūrio.

Šio disertacinio darbo naujumas pasireiškia tuo, kad kibernetinio saugumo valdymas tiriamas kompleksiškai, jungiant technologinius, organizacinius, procesinius

ir teisinius e. sveikatos sistemos aspektus. Atlikus mokslinės literatūros, tarptautinių standartų ir praktinių e. sveikatos sistemų atvejų analizę, disertacijoje identifikuojami specifiniai kibernetinio saugumo valdymo pažeidžiamumai, rizikos veiksniai ir e. sveikatos infrastruktūros sąveikos trūkumai, turintys esminės įtakos sistemos patikimumui. Tyrimo metu taip pat analizuojamos tarptautinės e. sveikatos sistemų kibernetinių incidentų praktikos, leidžiančios įvertinti tarptautiniuose tyrimuose ir praktikoje išryškėjančias tendencijas ir išskirti ypač pažeidžiamus sistemos komponentus. Skirtingai nei egzistuojantys kibernetinio saugumo modeliai, šiame darbe siūlomas modelis integruoja strateginį, organizacinį, procesinį ir technologinį valdymo lygmenis būtent e. sveikatos sistemos ekosistemos kontekste ir yra empiriškai pagrįstas ekspertinio tyrimo duomenimis nacionaliniu kontekstu.

Darbo praktinis reikšmingumas atsiskleidžia keliais aspektais. Pirma, disertacijoje pateikiamas kibernetinio saugumo valdymo modelis gali būti tiesiogiai taikomas e. sveikatos sistemos tobulinimo, projektavimo ir administravimo procesuose, siekiant sudaryti prielaidas mažinti infrastruktūros pažeidžiamumą ir stiprinti sistemos atsparumą kibernetinėms grėsmėms. Antra, modelio vertinimo kriterijai ir struktūriniai elementai gali būti naudojami sveikatos priežiūros įstaigų vadovams ir politikos formuotojams priimant sprendimus dėl saugumo valdymo brandos didinimo, resursų paskirstymo ir rizikų mažinimo priemonių planavimui. Trečia, tyrimo rezultatai suteikia metodologinį pagrindą e. sveikatos politikos formavimui, standartų adaptavimui ir kibernetinio saugumo valdymo principų integravimui į strateginio valdymo dokumentus.

Disertacijoje siūlomas modelis gali būti taikomas ne tik e. sveikatos sistemos kūrimo ir eksploatavimo etapuose, bet ir atliekant periodinius e. sveikatos sistemos saugumo vertinimus, planuojant infrastruktūros modernizavimą bei stiprinant organizacijų pasirengimą reaguoti į kibernetines grėsmes. Tokiu būdu tyrimas prisideda prie e. sveikatos sistemos tvarios plėtros ir sudaro prielaidas saugesnių, patikimesnių ir visuomenės pasitikėjimą užtikrinančių e. sveikatos paslaugų plėtojimui Lietuvoje.

Darbo struktūra

Disertacinį darbą sudaro trys tarpusavyje logiškai susijusios dalys.

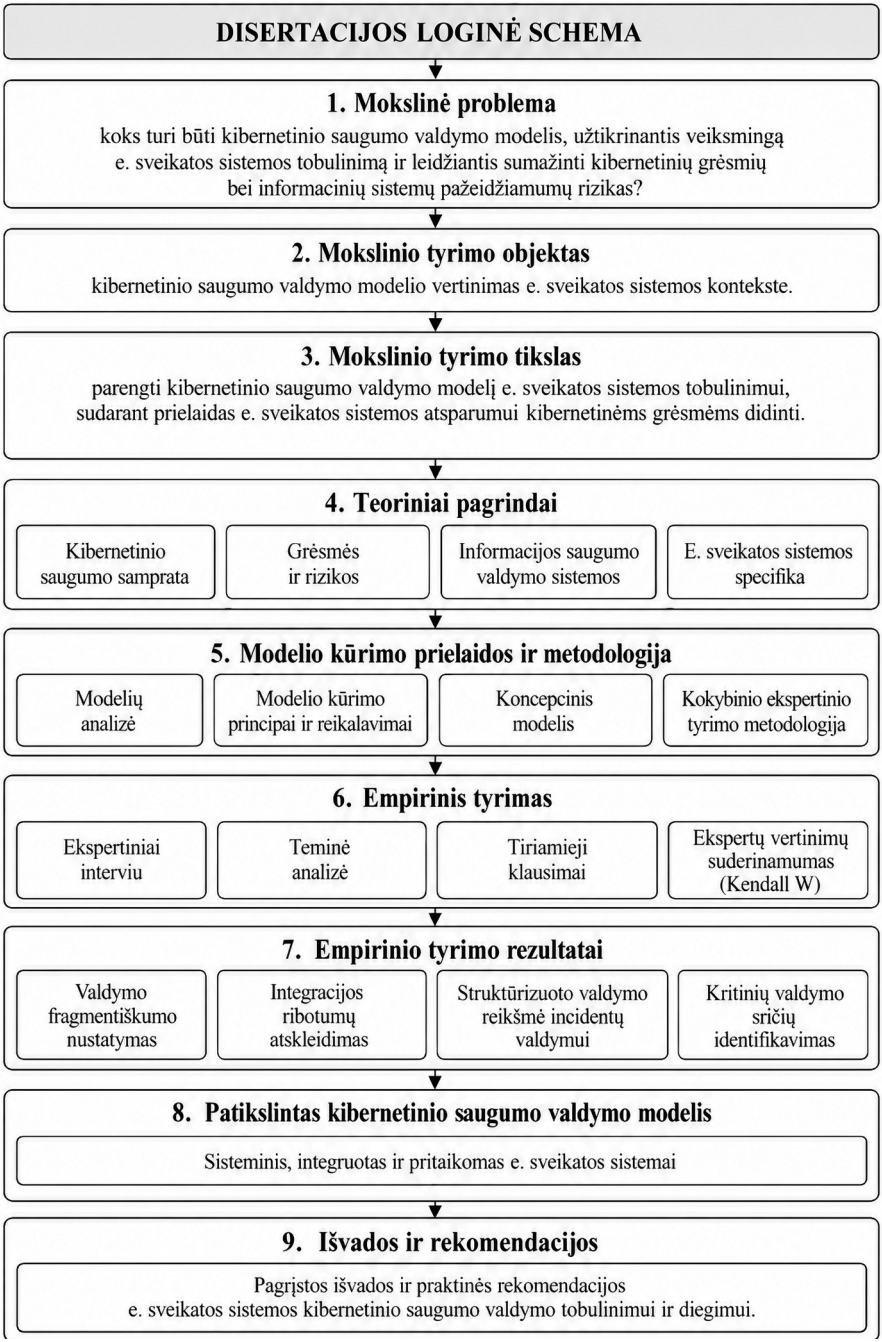
Pirmojoje disertacijos dalyje nagrinėjami kibernetinio saugumo valdymo teoriniai aspektai. Joje analizuojama kibernetinio saugumo sampratos raida, pagrindiniai principai ir tikslai, aptariamos šiuolaikinės kibernetinės grėsmės ir rizikos, ypač aktualios e. sveikatos sektoriui. Taip pat nagrinėjamos informacijos saugumo valdymo sistemos, tarptautiniai standartai (ISO/IEC 27001, 27005), TIS2 direktyvos reikalavimai bei kibernetinio saugumo brandos modeliai. Pirmoji dalis sudaro teorinį pagrindą tolesnei modelio kūrimo ir empirinio vertinimo analizei.

Antrojoje disertacijos dalyje pateikiama kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui struktūros kūrimo koncepcija ir tyrimo metodologinis pagrindimas. Šioje dalyje analizuojami egzistuojantys teoriniai ir praktiniai kibernetinio saugumo valdymo modeliai, formuluojami modelio kūrimo principai ir

reikalavimai, apibrėžiamos prielaidos modelio struktūrai, valdymo lygiai, informacijos srautai ir atsakomybės paskirstymas. Taip pat detaliai pagrindžiama tyrimo metodologija, aprašomas tyrimo dizainas, ekspertų atranka, duomenų rinkimo priemonės bei taikyti duomenų analizės metodai.

Trečiojoje disertacijos dalyje pateikiami empirinio tyrimo rezultatai ir jų analizė. Šioje dalyje, remiantis ekspertinio interviu duomenimis, vertinamas kibernetinio saugumo valdymo lygis sveikatos įstaigose, identifikuojamos esminės kibernetinio saugumo spragos, analizuojamos rizikų ir incidentų valdymo praktikos bei atliekama teminė ekspertinių įžvalgų analizė. Gauti empiriniai rezultatai naudojami kritinių kibernetinio saugumo valdymo sričių identifikavimui ir siūlomo valdymo modelio tikslinimui. Atliekamas siūlomo kibernetinio saugumo valdymo modelio ekspertinis vertinimas. Joje analizuojamas modelio tinkamumas ir taikymo galimybės e. sveikatos sistemoje, įvertinamos modelio stiprybės ir ribotumai, suformuluojamos pagrįstos tobulinimo kryptys bei aptariamas modelio praktinis pritaikomumas skirtinguose organizaciniuose ir instituciniuose kontekstuose.

Darbo pabaigoje pateikiamos apibendrintos disertacijos išvados ir rekomendacijos, kuriose sistemiškai apžvelgiami pagrindiniai tyrimo rezultatai, įvertinamas pasiektas tyrimo tikslas ir suformuluojamos praktinės bei mokslinės rekomendacijos e. sveikatos sistemos kibernetinio saugumo valdymo tobulinimui (žr. 1 pav.).



1 pav. Disertacinio darbo struktūros loginė schema.

Šaltinis: sudaryta autorės

1. KIBERNETINIO SAUGUMO VALDYMO TEORINIAI ASPEKTAI

1.1. Kibernetinio saugumo samprata ir reikšmė

E. sveikatos sistemos šiandien laikomos viena reikšmingiausių skaitmeninės transformacijos krypčių sveikatos sektoriuje, nes jos sudaro prielaidas efektyvesniam paslaugų teikimui, duomenų mainams ir sprendimų priėmimui, pagrįstam dideliais duomenų kiekiais. Skaitmenizuojant sveikatos paslaugas, didėja informacinių sistemų tarpusavio sąveika, nuotolinių paslaugų apimtis ir priklausomybė nuo informacinių technologijų infrastruktūros, todėl kibernetinis saugumas tampa neatsiejama e. sveikatos sistemų patikimumo ir veiklos tęstinumo sąlyga. Mokslinėje literatūroje pabrėžiama, kad kibernetinio saugumo pažeidimai sveikatos sektoriuje gali turėti ne tik ekonominių ar reputacinių, bet ir tiesioginių neigiamų pasekmių pacientų saugumui bei visuomenės sveikatai (Kruse, Frederick, Jacobson, ir Monticone, 2017, Woods ir kt., 2005).

Kibernetinis saugumas apibrėžiamas kaip techninių, organizacinių ir procesinių priemonių visuma, skirta apsaugoti informacines sistemas, tinklus ir duomenis nuo neteisėtos prieigos, pažeidimų, sutrikdymo ar sunaikinimo (von Solms ir van Niekerk, 2013, Hopkin ir kt., 2018). E. sveikatos kontekste ši sąvoka įgauna papildomą reikšmę, nes čia tvarkomi itin jautrūs asmens sveikatos duomenys, o sistemų veikimo sutrikimai gali turėti kritinių pasekmių. Todėl kibernetinis saugumas e. sveikatos sistemose vis dažniau analizuojamas ne tik kaip technologinė problema, bet ir kaip kompleksinis valdymo reiškinys, apimantis strateginį planavimą, rizikos valdymą, teisinę atitiktį ir organizacinę kultūrą (Bada, Sasse, ir Nurse, 2019).

Pastaraisiais metais tarptautiniai tyrimai rodo, kad sveikatos sektorius tampa vienu dažniausių kibernetinių atakų taikinių. Jungtinėse Amerikos Valstijose atlikti tyrimai pabrėžia, jog sveikatos priežiūros organizacijos dažnai atsilieka diegiant pažangias saugumo priemones, palyginti su finansų ar gynybos sektoriumi, nors jų valdomų duomenų vertė juodojoje rinkoje yra itin didelė (McLeod ir Dolezel, 2018). Dirbtinio intelekto taikymas kibernetinio saugumo stiprinimui tampa viena perspektyviausių krypčių. Mašininio mokymosi algoritmai gali efektyviai identifikuoti anomalijas didelio masto sveikatos duomenų rinkiniuose ir reikšmingai sumažinti duomenų nutekinimo riziką.

Kartu Jungtinėse Amerikos Valstijose didelis dėmesys skiriamas sisteminiam kibernetinio atsparumo didinimui. Nacionalinio standartų ir technologijų instituto (NIST) parengtuose tyrimuose akcentuojama, kad e. sveikatos sistemų saugumas turi būti grindžiamas rizikos valdymo ciklu, apimančiu grėsmių identifikavimą, prevenciją, reagavimą ir atkūrimą (NIST, 2014, 2020). Tokia koncepcija pabrėžia, jog absoliutus saugumas nėra pasiekiamas, tačiau organizacijos gebėjimas greitai atkurti paslaugas po incidento yra esminis veiksnys.

Europos Sąjungoje kibernetinio saugumo reikšmė e. sveikatos srityje glaudžiai siejama su teisės aktų harmonizavimu ir standartizavimu. Bendrasis duomenų apsaugos reglamentas (BDAR) iš esmės pakeitė požiūrį į asmens sveikatos duomenų apsaugą,

įtvirtindamas griežtesnius reikalavimus duomenų tvarkymo skaidrumui, saugumui ir atsakomybei. Leideno universiteto mokslininkų tyrimas atskleidė, kad BDAR įgyvendinimas paskatino e. sveikatos sistemų saugumo procedūrų formalizavimą, tačiau taip pat parodė, jog praktinis reglamento taikymas vis dar susiduria su organizaciniais ir technologiniais iššūkiais.

Azijos regione, pasižyminčiame sparčia e. sveikatos sistemų plėtra, kibernetinis saugumas dažnai siejamas su inovatyvių technologijų taikymu. Pietų Korėjos mokslininkai pasiūlė blokų grandinių (angl. *blockchain*) technologija pagrįstus sprendimus, skirtus elektroninių medicininių įrašų apsaugai, ir nustatė, kad decentralizuota duomenų architektūra reikšmingai sumažina neteisėtos prieigos riziką (Abunadi ir Kumar, 2021). Tačiau tyrėjai taip pat pabrėžia, kad blokų grandinės (angl. *blockchain*) technologijos diegimas reikalauja aiškios valdymo struktūros ir papildomų resursų.

Apibendrinant tarptautinių tyrimų rezultatus, galima teigti, kad kibernetinis saugumas e. sveikatos sistemose yra daugialypis reiškinys, reikalaujantis technologinių inovacijų, teisinio reguliavimo, organizacinio valdymo ir nuolatinio kompetencijų ugdymo dermės. Dirbtinio intelekto ir blokų grandinių (angl. *blockchain*) technologijos vertinamos kaip perspektyvios priemonės, tačiau be nuoseklaus valdymo modelio jų potencialas išlieka ribotas. Todėl mokslinėje literatūroje vis dažniau pabrėžiamas poreikis kurti ir vertinti kibernetinio saugumo valdymo modelius, pritaikytus būtent e. sveikatos sistemos tobulinimui, atsižvelgiant į jos technologinį sudėtingumą ir socialinę reikšmę (Garcia-Perez, 2023, Botsis ir kt. 2010).

Lietuvos kontekste e. sveikatos sistemų kibernetinis saugumas tampa vis aktualesniu klausimu dėl didėjančio skaitmenizacijos masto, tarptautinių duomenų mainų ir augančių kibernetinių grėsmių. Nors nacionaliniu lygmeniu priimami teisės aktai ir strateginiai dokumentai sudaro pagrindą saugumo užtikrinimui, mokslinėje literatūroje pabrėžiama, kad praktinis kibernetinio saugumo valdymo modelių pritaikymas e. sveikatos srityje vis dar reikalauja gilesnių empirinių tyrimų ir sisteminio vertinimo. Šios aplinkybės pagrindžia būtinybę tirti kibernetinio saugumo valdymo sampratą ir reikšmę e. sveikatos sistemos tobulinimo kontekste.

1.1.1. Kibernetinio saugumo sąvokos raida

Kibernetinio saugumo sąvokos raida yra neatsiejama nuo informacinių technologijų plėtros, sistemų teorijos formavimosi ir organizacijų veiklos skaitmeninimo procesų. Šiuolaikinėje visuomenėje kibernetinis saugumas tapo fundamentalia sąlyga užtikrinant skaitmeninių paslaugų patikimumą, ypač tokiose srityse kaip e. sveikata, kur tvarkomi itin jautrūs asmens duomenys (ENISA, 2023).

Istoriškai kibernetinio saugumo sampratos ištakos siekia kibernetikos mokslo atsiradimą XX amžiaus viduryje. Terminas „kibernetika“ pirmą kartą sistemingai pavartotas Norberto Wienerio veikale *Cybernetics: Or Control and Communication in the Animal and the Machine*, kuriame kibernetika apibrėžiama kaip valdymo ir ryšių sistemų gyvuose organizmuose bei mašinose mokslas (Wiener, 1948). Šis požiūris pabrėžė informacijos apdorojimo, grįžtamojo ryšio ir kontrolės svarbą, sudariusią pagrindą

vėlesniems informacijos ir kibernetinio saugumo tyrimams.

Kibernetikos idėjas toliau plėtojo Ashby, akcentavęs sistemų gebėjimą palaikyti stabilumą kintančioje aplinkoje, kas šiandien siejama su atsparumo koncepcija kibernetinio saugumo srityje (Ashby, 1956; Linkov ir kt., 2019). Nors ankstyvuosiuose darbuose saugumas nebuvo išskiriamas kaip atskira sąvoka, sistemų jautrumas trikdžiams ir kontrolės mechanizmų svarba tapo prielaidomis saugumo problematikos formavimuisi.

Vystantis kompiuterinėms sistemoms ir tinklams, ypač išpopuliarėjus interneto naudojimui, saugumas pradėtas suvokti kaip praktinė būtinybė. XX amžiaus pabaigoje saugumo sprendimai daugiausia buvo orientuoti į technines priemones, tokias kaip šifravimas, autentifikavimas ir tinklų apsauga (Anderson, 2020). Tačiau sudėtingėjant informacinių sistemų integracijai į organizacijų veiklos procesus, tapo akivaizdu, kad technologinis požiūris yra nepakankamas (von Solms ir van Niekerk, 2013).

Šiuolaikinėje mokslinėje literatūroje kibernetinis saugumas apibrėžiamas kaip kompleksinis, tarpdisciplininis reiškinys. Nacionalinis standartų ir technologijų institutas (NIST) kibernetinį saugumą apibrėžia kaip procesų, technologijų ir kontrolės priemonių visumą, skirtą apsaugoti sistemas, tinklus ir duomenis nuo kibernetinių grėsmių (NIST, 2018). Naujausioje ISO/IEC 27032:2023 redakcijoje kibernetinis saugumas apibrėžiamas kaip gairių ir praktikų visuma, skirta apsaugoti skaitmeninę aplinką nuo kibernetinių grėsmių, užtikrinant informacijos konfidencialumą, vientisumą ir prieinamumą (ISO/IEC, 2023).

Kartu su kibernetinio saugumo sąvoka evoliucionavo ir kitos sąvokos susijusios su kibernetiniu saugumu. Kibernetinė grėsmė apibrėžiama kaip potencialus veiksnys ar įvykis, galintis išnaudoti pažeidžiamumus ir sukelti žalą organizacijai ar visuomenei (ISO/IEC, 2022). Kibernetinis incidentas suprantamas kaip faktinis ar galimas įvykis, pažeidžiantis informacijos saugumo politiką ar turintis poveikį paslaugų teikimo tęstinumui (NIST, 2012; ENISA, 2022). Kibernetinė gynyba apima koordinuotų prevencijos, aptikimo, reagavimo ir atkūrimo priemonių visumą, kuri tampa ypač aktuali kritinės infrastruktūros, įskaitant e. sveikatos sistemas, apsaugai (NATO CCDCOE, 2022).

Apibendrinant galima teigti, kad kibernetinio saugumo sąvoka per kelis dešimtmečius išsivystė iš siauro, technologinio termino į kompleksinę, tarpdisciplininę kategoriją, apimančią technologinius, organizacinius ir strateginius aspektus (von Solms ir van Niekerk, 2013; Craigen ir kt., 2014). Skirtingų autorių ir institucijų pateikiami apibrėžimai atskleidžia nuoseklų perėjimą nuo sistemų kontrolės ir techninės apsaugos prie holistinio kibernetinio saugumo valdymo, integruojančio rizikos valdymą, organizacinį atsparumą ir žmogiškąjį veiksnį (Linkov ir kt., 2019; ENISA, 2023).

1.1.2. Kibernetinio saugumo pagrindiniai principai ir tikslai

Kibernetinio saugumo principai ir tikslai formuoja normatyvinį ir metodologinį pagrindą, kuriuo remiasi šiuolaikinės organizacijos, siekdamos apsaugoti savo informacinius išteklius, užtikrinti veiklos tęstinumą ir valdyti kylančias skaitmenines rizikas. Kaip parodyta ankstesniame poskyryje, kibernetinio saugumo sąvoka perėjo

nuo siauro techninio supratimo prie kompleksinio, tarpdisciplininio reiškinio. Ši raida lėmė ir kibernetinio saugumo principų transformaciją – nuo technologinių kontrolės mechanizmų link strateginių valdymo nuostatų (von Solms ir van Niekerk, 2013; Craigen ir kt., 2014).

Vienas universaliausių ir plačiausiai pripažintų kibernetinio saugumo principų yra konfidencialumo, vientisumo ir prieinamumo (CIA) triada, kuri išlieka pagrindiniu atskaitos tašku tiek moksliniuose tyrimuose, tiek tarptautiniuose standartuose (Whitman ir Mattord, 2021; ISO/IEC, 2022). Konfidencialumo principas siejamas su informacijos apsauga nuo neautorizuotos prieigos, vientisumas – su duomenų tikslumo, patikimumo ir nepakitimo užtikrinimu, o prieinamumas – su sistemų gebėjimu užtikrinti nenutrūkstamą paslaugų teikimą. E. sveikatos sistemų kontekste ši triada įgyja ypatingą reikšmę, nes bet kurios iš šių dimensijų pažeidimas gali turėti tiesioginių pasekmių pacientų saugumui ir visuomenės pasitikėjimui e. sveikatos paslaugomis (Kruse ir kt., 2017).

Vis dėlto šiuolaikinėje literatūroje pabrėžiama, kad CIA triada yra būtina, tačiau nepakankama sąlyga veiksmingam kibernetinio saugumo valdymui. Dėl šios priežasties ji papildoma tokiais principais kaip atsparumas, patikimumas, atskaitomybė ir nuolatinis tobulinimas (Linkov ir kt., 2019; ENISA, 2023). Atsparumo principas akcentuoja organizacijos gebėjimą veikti neapibrėžtomis sąlygomis, laiku aptikti kibernetinius incidentus, sumažinti jų poveikį ir atkurti veiklą po sutrikimų. Sveikatos sektoriuje šis principas yra ypač svarbus, nes paslaugų nutraukimas ar sistemų neveikimas gali kelti grėsmę gyvybei.

Kitas esminis kibernetinio saugumo principas yra rizika grįstas požiūris, kuris laikomas kertiniu tiek informacijos, tiek kibernetinio saugumo valdymo elementu. Pagal ISO/IEC 27005:2022, saugumo priemonės turi būti parenkamos ne abstrakčiai, o remiantis sistemingu rizikų identifikavimu, analize ir vertinimu, atsižvelgiant į galimą poveikį organizacijos tikslams (ISO/IEC, 2022). Moksliniai tyrimai rodo, kad rizika grįstas valdymas leidžia organizacijoms efektyviau paskirstyti ribotus išteklius ir sutelkti dėmesį į kritiškiausias grėsmes (Aven ir Zio, 2016; Hubbard ir Seiersen, 2016).

Rizikos valdymo principas glaudžiai susijęs su prevencijos ir ankstyvo aptikimo nuostata. Šiuolaikiniai kibernetinio saugumo modeliai pabrėžia, kad efektyvus saugumo valdymas turi būti orientuotas ne tik į reagavimą po incidento, bet ir į grėsmių prevenciją, ankstyvą aptikimą bei nuolatinį grėsmių stebėjimą (NIST, 2023; Floridi ir Taddeo, 2016). Tyrimai rodo, kad organizacijos, kurios diegia nuoseklias grėsmių aptikimo ir reagavimo sistemas, pasiekia aukštesnį saugumo brandos lygį ir patiria mažesnius nuostolius dėl kibernetinių incidentų (Singer ir Friedman, 2014).

Svarbią vietą kibernetinio saugumo principuose užima organizacinis ir žmogiškasis veiksnys, kuris mokslinėje literatūroje dažnai įvardijamas kaip viena silpniausių saugumo grandžių (Parsons ir kt., 2015; Alshaikh, 2020). Saugumo kultūros formavimas, darbuotojų kompetencijų stiprinimas ir aiškus atsakomybių paskirstymas yra būtinos sąlygos veiksmingam saugumo priemonių taikymui. Sveikatos sektoriuje, kuriame e. sveikatos sistemomis naudojasi skirtingų profesinių grupių atstovai, žmogiškasis veiksnys tampa ypač reikšmingas (Kruse ir kt., 2017; ENISA, 2023).

Šiuolaikinėje teorijoje taip pat akcentuojamas holistinis ir integruotas požiūris į kibernetinį saugumą, kuriame technologiniai sprendimai derinami su vadybiniais ir teisiniais mechanizmais. Tarptautiniai standartai, tokie kaip ISO/IEC 27001:2022 ir ISO/IEC 27002:2022, pabrėžia nuolatinio tobulinimo ciklo (angl. *Plan Do Check Act*) svarbą, leidžiančią sistemingai vertinti saugumo priemonių efektyvumą ir jas adaptuoti kintančiai grėsmių aplinkai (ISO/IEC, 2022). Šis principas ypač aktualus e. sveikatos sistemoms, kurios pasižymi aukštu technologiniu dinamiškumu ir tarporganizacine sąveika.

Kibernetinio saugumo tikslai, remiantis aptartais principais, apibrėžiami kaip siekis apsaugoti informacinius ir technologinius išteklius, užtikrinti paslaugų tęstinumą, sumažinti kibernetinių incidentų tikimybę ir poveikį, didinti organizacijų atsparumą bei stiprinti suinteresuotųjų šalių pasitikėjimą (ENISA, 2023; OECD, 2008). Šie tikslai turi būti derinami su organizacijos strateginiais tikslais ir veiklos prioritetais.

Technologinės inovacijos, tokios kaip dirbtinis intelektas literatūroje vertinamos kaip potencialios priemonės kibernetinio saugumo tikslams pasiekti, tačiau pabrėžiama, kad jų efektyvumas priklauso nuo integracijos į bendrą valdymo sistemą. Šių principų reikšmė disertacijai yra ta, kad jie leidžia kibernetinį saugumą traktuoti ne kaip atskirų priemonių sąrašą, o kaip valdymo logiką, kuri vėliau perkeliama į modelio struktūrą.

1.1.3. Kibernetinio saugumo svarba skaitmenizuotoje visuomenėje

Pastaraisiais dešimtmečiais skaitmenizacija tapo esminiu visuomenės raidos veiksniu, lemiančiu ne tik technologinius, bet ir organizacinius bei socialinius pokyčius. Skaitmeninės sistemos vis plačiau integruojamos į viešąsias paslaugas, ekonomiką ir kasdienę žmonių veiklą, todėl jų patikimumas ir saugumas tampa kritiškai svarbūs ne pavienėms organizacijoms, bet visai visuomenei. Mokslinėje literatūroje pabrėžiama, kad kibernetinis saugumas šiuolaikinėmis sąlygomis nebėra siaurai suprantamas kaip techninių apsaugos priemonių rinkinys – jis vis dažniau vertinamas kaip viena iš pamatinių skaitmenizuotos visuomenės funkcionavimo prielaidų (Vial, 2019).

Augantis informacinių sistemų tarpusavio susietumas lemia tai, kad kibernetiniai incidentai gali turėti neproporcingai didelį poveikį. Vienos sistemos sutrikimas neretai paveikia platesnį paslaugų tinklą, o pasekmės pasireiškia ne tik technologiniu, bet ir socialiniu lygmeniu. Tokios situacijos ypač aktualios sektoriuose, kuriuose skaitmeninės sistemos yra tiesiogiai susijusios su gyvybiškai svarbiomis funkcijomis, pavyzdžiui, sveikatos priežiūra, energetika ar finansinėmis paslaugomis. Tyrimai rodo, kad šiose srityse kibernetinio saugumo problemos vis dažniau suvokiamos kaip sisteminės rizikos, o ne pavieniai techniniai nesklandumai (Linkov ir Trump, 2019).

Tarptautiniu mastu sveikatos sektorius dažnai išskiriamas kaip vienas jautriausių skaitmeninės transformacijos sričių. E. sveikatos įrašų, nuotolinių paslaugų ir integruotų klinikinių informacinių sistemų plėtra sudaro prielaidas efektyvesniam paslaugų teikimui. Empiriniai tyrimai rodo, kad net ir trumpalaikiai kibernetiniai sutrikimai sveikatos sektoriuje gali turėti ilgalaikių pasekmių, susijusių su paslaugų prieinamumu,

pacientų sauga ir pasitikėjimu institucijomis (Jalali ir Kaiser, 2018). Dėl šios priežasties kibernetinis saugumas šioje srityje tampa neatsiejama kokybiškos sveikatos priežiūros dalimi.

Svarbus kibernetinio saugumo aspektas skaitmenizuotoje visuomenėje yra pasitikėjimas skaitmeninėmis paslaugomis. Tyrimai rodo, kad vartotojų elgsena ir jų sprendimas naudotis skaitmeninėmis sistemomis glaudžiai susijęs su suvokiamu saugumo lygiu. Kibernetiniai incidentai, ypač susiję su jautrių duomenų pažeidimais, gali turėti ilgalaikį poveikį visuomenės požiūriui į skaitmenines iniciatyvas, net ir tada, kai techninės problemos vėliau yra išsprendžiamos (Martin ir kt., 2017). Ši aplinkybė ypač reikšminga sveikatos sektoriuje, kur pasitikėjimas yra būtina sąlyga sėkmingam e. paslaugų taikymui.

Pastaruoju metu moksliniuose tyrimuose vis daugiau dėmesio skiriama kibernetinio atsparumo sampratai, kuri papildo tradicinį kibernetinio saugumo supratimą. Atsparumas apima organizacijų gebėjimą prisitaikyti prie kintančios grėsmių aplinkos, veiksmingai reaguoti į incidentus ir užtikrinti esminių funkcijų tęstinumą. Šis požiūris ypač aktualus sudėtingose informacinėse sistemose, tokiose kaip e. sveikatos infrastruktūra, kur visiškas incidentų eliminavimas laikomas praktiškai nepasiekiamu tikslu (Parsons ir kt., 2014).

Ne mažiau reikšmingas ir žmogiškasis veiksnys, kuris skaitmenizuotoje visuomenėje dažnai tampa silpnąja kibernetinio saugumo grandimi. Tyrimai rodo, kad technologinės apsaugos priemonės ne visuomet kompensuoja organizacines spragas, nepakankamą darbuotojų pasirengimą ar saugumo kultūros stoką. Sveikatos sektoriuje ši problema išryškėja dėl didelio darbo tempo, būtinybės greitai pasiekti informaciją ir ribotų galimybių skirti laiko saugumo procedūrų laikymuisi (Parsons ir kt., 2017). Dėl to kibernetinis saugumas vis dažniau analizuojamas kaip socio-techninė problema, reikalaujanti integruoto požiūrio.

Atsižvelgiant į šias aplinkybes, kibernetinio saugumo svarba skaitmenizuotoje visuomenėje tampa akivaizdi. Jis veikia ne tik kaip techninė apsaugos funkcija, bet ir kaip būtina sąlyga paslaugų tęstinumui, visuomenės pasitikėjimui ir kritinių sistemų stabilumui užtikrinti. E. sveikatos sistemų kontekste tai sudaro prielaidas tolesnei kibernetinių grėsmių ir rizikų analizei, kuri yra būtina siekiant suprasti, su kokiais iššūkiais susiduria šiuolaikinės skaitmeninės sveikatos ekosistemos.

1.2. Kibernetinio saugumo grėsmės ir rizikos

Skaitmenizuotos visuomenės kontekste kibernetinio saugumo reikšmė neatsiejama nuo nuolat didėjančios kibernetinių grėsmių ir rizikų įvairovės bei jų poveikio kritinėms informacinėms sistemoms. Spartus informacinių ir ryšių technologijų vystymasis, duomenų mainų intensyvėjimas bei skaitmeninių paslaugų integracija į esminius visuomenės procesus sukuria aplinką, kurioje kibernetiniai incidentai tampa ne pavieniais techniniais sutrikimais, o sisteminėmis grėsmėmis organizacijų veiklos tęstinumui ir visuomenės saugumui (Rios Insua ir kt., 2019). Dėl šios priežasties kibernetinio saugumo problematika vis dažniau analizuojama per grėsmių ir rizikų

valdymo prizmę, siekiant suprasti ne tik incidentų pasekmes, bet ir jų kilmės priežastis bei struktūrinius veiksnius.

Mokslinėje literatūroje pabrėžiama, kad kibernetinės grėsmės nėra statiškas reiškinys. Priešingai, jos nuolat evoliucionuoja, prisitaikydamos prie technologinės pažangos, organizacinių struktūrų transformacijos ir naudotojų elgsenos pokyčių. Šiuolaikinės kibernetinės grėsmės pasižymi hibridiniu pobūdžiu, apimančiu tiek techninius pažeidžiamumus, tiek socialinės inžinerijos metodus, tiek organizacinių procesų spragas (Bada ir Nurse, 2019, Caralli ir kt., 2012, De Bruijn ir kt., 2017). Tokia grėsmių dinamika lemia, kad vien techninėmis priemonėmis grindžiamas saugumo užtikrinimas tampa nepakankamas, o dėmesys vis dažniau sutelkiamas į sisteminį, holistinį ir rizikomis grindžiamą požiūrį į kibernetinį saugumą.

Kibernetinė rizika mokslinėje literatūroje analizuojama kaip tikėtinas neigiamas poveikis, kylantis realizavus tam tikras grėsmes konkrečioje sistemoje ar organizacinėje aplinkoje. Skirtingai nei grėsmės, kurios gali egzistuoti nepriklausomai nuo konkretaus konteksto, rizika yra kontekstinė ir priklauso nuo sistemos pažeidžiamumo lygio, taikomų apsaugos priemonių brandos bei galimų pasekmių masto (Sheikh ir kt., 2021). Tokiu būdu rizika tampa ne vien techniniu, bet ir valdymo bei sprendimų priėmimo klausimu, susijusiu su prioritetų nustatymu, išteklių paskirstymu ir toleruotino rizikos lygio apibrėžimu.

Ypač sudėtingas rizikų pobūdis atsiskleidžia organizacijose, veikiančiose itin reguliuojamose ir kompleksiškose aplinkose, tokiose kaip sveikatos sektorius. Tyrimai rodo, kad šiose sistemose kibernetinės rizikos neapsiriboja vien informacinėmis sistemomis ar duomenų saugumo aspektais, bet apima ir klinikinius procesus, pacientų saugą bei paslaugų prieinamumą (Sheikh ir kt., 2021). Tai suponuoja poreikį atsisakyti universalių, bendrinio pobūdžio rizikų vertinimo modelių ir taikyti sektoriui pritaikytas rizikų analizės metodologijas.

Kibernetinių grėsmių analizė taip pat atskleidžia, kad vis dažniau grėsmės kyla ne iš vieno izoliuoto šaltinio, o formuojasi dėl kelių veiksnių sąveikos. Technologinės spragos, nepakankamas procesų formalizavimas, žmogiškosios klaidos ar netinkami valdymo sprendimai kartu sudaro palankias sąlygas incidentams atsirasti. Tokios kompleksinės situacijos ypač būdingos didelėms, tarpusavyje integruotoms informacinėms sistemoms, veikiančioms kaip ekosistemos, o ne atskiri techniniai sprendimai (Boyes ir kt., 2018). Ši aplinkybė pabrėžia, kad kibernetinės grėsmės turi būti vertinamos ne fragmentiškai, bet sistemiškai.

Lietuvos ir tarptautiniuose tyrimuose vis dažniau akcentuojama, kad tradicinis požiūris į kibernetinį saugumą, orientuotas vien į technologines apsaugos priemones, negeba adekvačiai valdyti sudėtingų socio-techninių grėsmių. Limba ir bendraautoriai teigia, kad efektyvus kibernetinio saugumo valdymas turi būti grindžiamas integruotais modeliais, apimančiais strateginį valdymą, organizacinius procesus, atsakomybių paskirstymą ir rizikų analizę, o ne vien techninių sprendimų diegimą (Limba ir kt., 2017). Tokia pozicija leidžia kibernetines grėsmes suvokti kaip valdymo, o ne vien informacinių technologijų problemą.

Kibernetinių grėsmių ir rizikų analizė tampa būtinu teoriniu pagrindu, siekiant

kurti veiksmingus kibernetinio saugumo valdymo modelius. Be aiškaus supratimo apie grėsmių pobūdį, jų klasifikaciją ir rizikų formavimosi mechanizmus, neįmanoma pagrįstai vertinti saugumo lygio ar planuoti jo tobulinimo priemonių. Tai ypač aktualu e. sveikatos sistemų kontekste, kuriame kibernetiniai incidentai gali turėti tiesioginį poveikį ne tik organizacijų veiklai, bet ir pacientų saugai bei visuomenės pasitikėjimui sveikatos sistema. Todėl tolesniuose šio skyriaus poskyriuose detaliau nagrinėjama kibernetinių incidentų klasifikacija, rizikų veiksniai e. sveikatos srityje bei galimos kibernetinių incidentų pasekmės, vedančios į vėlesnę empirinio tyrimo ir kibernetinio saugumo valdymo modelio kūrimo dalį.

1.2.1. Kibernetinių incidentų klasifikacija

Kibernetinių incidentų analizė yra vienas esminių kibernetinio saugumo valdymo elementų, nes nuo tinkamo incidentų supratimo ir sisteminimo priklauso tiek rizikų vertinimo tikslumas, tiek pasirenkamų saugumo priemonių pagrįstumas. Mokslinėje literatūroje pabrėžiama, kad kibernetiniai incidentai pasižymi didele įvairove, todėl jų klasifikavimas yra sudėtingas, tačiau būtinas siekiant užtikrinti nuoseklų saugumo valdymą organizacijose (Howard, 1997; Singer ir Friedman, 2014).

Ankstyvieji kibernetinių incidentų klasifikavimo modeliai daugiausia rėmėsi techniniais kriterijais, tokiais kaip atakos tipas ar panaudotos priemonės. Šiuose modeliuose incidentai buvo skirstomi į kenkėjiškų programų atakas, paslaugų trikdymo (angl. *Denial of Service*) atvejus, neteisėtos prieigos incidentus ar duomenų pakeitimus. Nors toks požiūris leido standartizuoti techninę incidentų analizę, jis nepakankamai atskleidė platesnį incidentų poveikį organizacijoms ir jų veiklos procesams (Howard, 1997; Kjaerland, 2006).

Vėlesniuose tyrimuose klasifikavimo požiūris buvo išplėstas, įtraukiant incidentų tikslus ir pasekmes. Mokslininkai pradėjo diferencijuoti incidentus pagal jų siekiamą naudą, pavyzdžiui, finansinę naudą, duomenų vagystę, paslaugų sutrikdymą ar reputacinę žalą. Tokia klasifikacija leido geriau suprasti atakų motyvus ir taikyti tikslingesnes prevencijos priemones (Kjaerland, 2006; Greitzer ir kt., 2014).

Didėjant informacinių sistemų sudėtingumui ir jų integracijai į organizacijų veiklos procesus, vis daugiau dėmesio skiriama daugiamatėms kibernetinių incidentų klasifikacijoms. Šiuose modeliuose incidentai vertinami ne tik techniniu, bet ir organizaciniu, procesiniu bei žmogiškuoju lygmenimis. Tokia perspektyva ypač aktuali sveikatos sektoriuje, kuriame kibernetiniai incidentai gali turėti tiesioginį poveikį paslaugų teikimui ir pacientų saugumui (Shameli-Sendi ir kt., 2016; Sommestad ir kt., 2019).

Siekiant sistemiškai palyginti mokslinėje literatūroje taikomus kibernetinių incidentų klasifikavimo požiūrius, toliau pateikiama lentelė, apibendrinanti dažniausiai cituojamus autorių siūlomus klasifikavimo kriterijus ir jų taikymo kontekstus.

1 lentelė. Kibernetinių incidentų klasifikavimo požiūrių palyginimas

Autorius (-iai)	Klasifikavimo pagrindas	Išskiriami incidentų tipai	Taikymo kontekstas
Howard (1997)	Techninis pobūdis	Kenkėjiškos programos, paslaugų trikdymas, neteisėta prieiga	Techninė incidentų analizė
Kjaerland (2006)	Incidento tikslas	Duomenų vagystė, finansinė nauda, sabotažas	Organizacijų saugumo analizė
Greitzer ir kt. (2014)	Grėsmės kilmė	Vidiniai ir išoriniai incidentai	Žmogiškųjų veiksnių vertinimas
Shameli-Sendi ir kt. (2016)	Daugiamatis modelis	Techniniai, organizaciniai, procesiniai incidentai	Kompleksinės socio-techninės sistemos
Singer ir Friedman (2014)	Poveikis organizacijai	Operaciniai, reputaciniai, teisiniai incidentai	Kritinė infrastruktūra
Sommestad ir kt. (2019)	Klasifikavimo pakankamumas	Kombinuoti incidentų tipai	Metodologinė analizė
Kruse ir kt. (2017)	Poveikis sveikatos paslaugoms	Klinikiniai, administraciniai, asmens duomenų saugumo pažeidimai	Sveikatos sektorius

Šaltinis: sudaryta autorės remiantis Howard (1997), Kjaerland (2006), Greitzer ir kt. (2014), Shameli-Sendi ir kt. (2016), Singer ir Friedman (2014), Sommestad ir kt. (2019), Kruse ir kt. (2017)

Lentelėje pateikti duomenys rodo, kad nėra vienos universalios kibernetinių incidentų klasifikacijos, tinkamos visoms sritims ir organizacijoms. Techniniai klasifikavimo modeliai yra naudingi identifikuojant atakų pobūdį, tačiau jie nepakankamai atspindi incidentų poveikį organizaciniams procesams ir paslaugų tęstinumui. Tuo tarpu daugiamatės klasifikacijos leidžia vertinti incidentus platesniame kontekste, integruojant technologinius, organizacinius ir žmogiškuosius aspektus.

Sveikatos sektoriuje tokia integruota incidentų klasifikacija yra ypač reikšminga, nes e. sveikatos sistemos veikia kaip sudėtingos socio-techninės ekosistemos. Kibernetiniai incidentai šioje srityje gali sukelti ne tik informacijos saugumo pažeidimus, bet ir sutrikdyti klinikinius procesus bei kelti grėsmę pacientų saugai. Todėl nuoseklus kibernetinių incidentų klasifikavimas yra svarbus tolesnei rizikų veiksnių analizei e. sveikatos sistemose, kuri nagrinėjama kitame poskyryje.

1.2.2. Rizikų veiksniai e. sveikatos srityje

Kibernetinių incidentų klasifikacija, aptarta ankstesniame poskyryje, sudaro pagrindą incidentų tipologijai ir jų pasekmių analizei, tačiau ji neatsako į klausimą, kodėl tam tikros sistemos ar sektoriai tampa labiau pažeidžiami nei kiti. Dėl šios priežasties moksliniuose tyrimuose vis didesnis dėmesys skiriamas rizikų veiksnių analizei, leidžiančiai identifikuoti struktūrines, technologines ir organizacines prielaidas, kurios didina kibernetinių incidentų tikimybę ir jų poveikį (Sommestad ir kt., 2019, Zubkov ir kt. 2025). E. sveikatos sistemų atveju ši analizė yra ypač reikšminga, nes kibernetinės rizikos čia tiesiogiai susijusios ne tik su informacijos saugumu, bet ir su sveikatos paslaugų teikimo tęstinumu bei pacientų sauga (Kruse ir kt., 2017).

Mokslinėje literatūroje e. sveikatos sistemos dažnai apibrėžiamos kaip sudėtingos sistemos, kuriose technologiniai komponentai yra glaudžiai susiję su organizaciniais procesais ir sprendimais (Sittig ir Singh, 2016). Toks požiūris leidžia suprasti, kad kibernetinės rizikos kyla ne vien dėl techninių spragų, bet ir dėl nepakankamo procesų suderinamumo, ribotų organizacinių gebėjimų bei žmogiškųjų klaidų. Todėl e. sveikatos sistemų rizikų vertinimas negali būti grindžiamas vien tik techniniais kriterijais, o turi apimti platesnį organizacinį ir institucinį kontekstą (Radanliev ir kt., 2018).

Vienas reikšmingiausių rizikų veiksnių e. sveikatos srityje yra informacinių sistemų architektūrinis sudėtingumas. Sveikatos priežiūros organizacijos dažnai eksploatuoja daugiakomponentes sistemas, kurios buvo kuriamos skirtingais laikotarpiais, vadovaujantis nevienodais technologiniais standartais. Tokia infrastruktūra pasižymi nevienodu saugumo brandos lygiu, o jos priežiūra ir atnaujinimas reikalauja didelių organizacinių ir finansinių išteklių (Fernandez-Aleman ir kt., 2013). Tyrimai rodo, kad būtent tokiose heterogeniškose aplinkose dažniausiai pasitaiko konfigūracijų klaidos, netinkamas prieigos teisių valdymas ir nepakankamas saugumo atnaujinimų diegimas (Alsubaei ir kt., 2017).

Technologinį sudėtingumą dar labiau didina spartus skaitmenizacijos procesas ir naujų technologijų integracija į e. sveikatos sistemas. Debesų kompiuterijos sprendimai, mobiliųjų sveikatos aplikacijų plėtra ir medicininių prietaisų interneto (angl. *IoMT*) diegimas išplečia funkcines galimybes, tačiau kartu padidina atakos apimtį ir apsunkina saugumo kontrolę (Rahmani ir kt., 2015). Moksliniai tyrimai pabrėžia, kad naujų technologijų diegimas dažnai lenkia organizacijų gebėjimą tinkamai įvertinti ir suvaldyti kylančias rizikas (Tariq ir kt., 2020).

Reikšmingą vaidmenį formuojant kibernetines rizikas atlieka ir e. sveikatos sistemose tvarkomų duomenų pobūdis. Elektroniniai sveikatos duomenys apima itin jautrią informaciją, kurios neteisėtas atskleidimas gali turėti ilgalaikių pasekmių asmens privatumui, socialinei padėčiai ir net profesinei veiklai (McLeod ir Dolezel, 2018). Dėl šios priežasties sveikatos sektorius yra nuolatinių tikslinių atakų objektas, ypač išpirkos reikalaujančių atakų kontekste, kai duomenų prieinamumas tampa spaudimo priemone (Coventry ir Branley, 2018; Jalali ir Kaiser, 2018, Jansen ir kt., 2011).

Organizaciniu lygmeniu kibernetines rizikas didina nepakankamai integruotas saugumo valdymas. Tyrimai rodo, kad sveikatos sektoriaus organizacijos dažnai

orientuojasi į teisės aktų laikymąsi, tačiau stokoja sistemingo rizikų valdymo, apimančio prevenciją, pasirengimą incidentams ir atkūrimo planavimą (Kellermann ir Jones, 2013; Ransbotham ir kt., 2012). Tokia situacija lemia, kad kibernetinis saugumas tampa reaguojančia, o ne proaktyvia funkcija, o tai didina incidentų poveikį ir atkūrimo kaštus.

Žmogiškasis veiksnys išlieka vienu sudėtingiausiu ir sunkiausiai kontroliuojamu rizikos šaltiniu. Empiriniai tyrimai rodo, kad didelė dalis kibernetinių incidentų yra susiję su netyčinėmis darbuotojų klaidomis, neatsargiu elgesiu su informacinėmis sistemomis ar nepakankamu grėsmių suvokimu (Parsons ir kt., 2017; Hadlington, 2017). Sveikatos sektoriuje ši problema dar labiau paaštrėja dėl didelio darbo krūvio, laiko trūkumo ir prioritetų, orientuotų į klinikinius sprendimus, o ne į informacijos saugumą (Ashenden ir Lawrence, 2016).

Papildomą rizikos dimensiją sudaro e. sveikatos sistemų tarpinstitucinis ir tarptautinis sąveikumas. Duomenų mainai tarp sveikatos priežiūros įstaigų, laboratorijų, draudimo bendrovių ir valstybinių registrų sudaro sudėtingą ekosistemą, kurioje vieno dalyvio saugumo spragos gali turėti grandininį poveikį visai sistemai (Bada ir Nurse, 2019; Radanliev ir kt., 2019; ENISA, 2021).

Apibendrinant e. sveikatos sistemoms būdingus rizikų veiksnius, galima išskirti jų tarpusavio priklausomybę. Technologiniai, organizaciniai ir žmogiškieji veiksniai veikia ne izoliuotai, o formuoja sudėtingą rizikų tinklą, kuris reikalauja integruoto kibernetinio saugumo valdymo požiūrio. Siekiant struktūruotai apibendrinti šiuos veiksnius, toliau pateikiama 2 lentelė.

2 lentelė. Kibernetinių rizikų veiksniai e. sveikatos sistemose ir jų poveikis

Rizikos veiksnių kategorija	Rizikos pobūdis	Tipinės apraiškos e. sveikatos sistemose	Galimas poveikis
Technologiniai	Sistemų sudėtingumas ir senėjimas	Pasenusios IS, sudėtinga integracija	Padidėjęs pažeidžiamumas
Duomenų	Didelis informacijos jautrumas	Asmens (sveikatos) duomenų saugumo pažeidimai	Ilgalaikį psichologinį, socialinį ir finansinį poveikį
Organizaciniai	Valdymo fragmentacija	Neaiškios atsakomybės, ribotas pasirengimas	Lėtas reagavimas
Žmogiškieji	Kompetencijų ir sąmoningumo stoka	Socialinės inžinerijos atakos	Incidentų eskalacija
Tarpinstituciniai	Priklausomybė nuo trečiųjų šalių	Grandininiai sutrikimai	Sisteminės krizės

Šaltinis: sudaryta autorės remiantis Kruse ir kt. (2017), Appari ir Johnson (2010), Rindfleisch (1997), Kwon ir Johnson (2014), Fernandez-Aleman ir kt. (2013), ISO/IEC 27005 (2018), ENISA (2021), Singer ir Friedman (2014)

Šie veiksniai formuojasi ir sąveikauja e. sveikatos sistemose, todėl būtina kurti integruotą, sisteminiu požiūriu grįstą kibernetinio saugumo valdymo modelį, kuris vėliau disertacijoje bus vertinamas empiriškai.

1.2.3. Kibernetiniai incidentai ir jų pasekmės

Kibernetiniai incidentai e. sveikatos sistemose neturėtų būti suprantami vien kaip pavieniai techniniai sutrikimai ar atskiri informacijos saugumo pažeidimai. Mokslinėje literatūroje vis dažniau pabrėžiama, kad tokie incidentai yra kompleksiniai reiškiniai, darantys daugialypį poveikį organizacijų veiklai, sveikatos paslaugų teikimo procesams ir platesnei visuomenės pasitikėjimo sistemai (Wirth, 2019, Dekker, 2017). Skaitmenizuotoje sveikatos priežiūros aplinkoje kibernetiniai incidentai tampa neatsiejama sisteminės rizikos dalimi, kurios pasekmės gali būti ilgalaikės, tarpusavyje susijusios ir sunkiai išmatuojamos (Martin ir kt., 2017).

Vienas esminių kibernetinių incidentų padarinių yra sveikatos paslaugų teikimo sutrikdymas. Empiriniai tyrimai rodo, kad incidentai, susiję su informacinių sistemų nepasiekiamumu, dažnai lemia planinių procedūrų atidėjimą, pacientų srautų valdymo problemas ir kritinių klinikinių sprendimų vėlavimą. Tokiose situacijose medicinos personalas priverstas pereiti prie rankinių ar alternatyvių procesų, kurie ne tik mažina veiklos efektyvumą, bet ir didina medicininių klaidų tikimybę (Coiera ir kt., 2012). Tai leidžia teigti, kad kibernetiniai incidentai e. sveikatos sistemoje tiesiogiai veikia pacientų saugą ir sveikatą, o neapsiriboja vien informacijos apsaugos aspektu.

Reikšminga incidentų pasekmių grupė siejama su duomenų vientisumo ir patikimumo pažeidimais. Mokslinėje literatūroje pabrėžiama, kad net ir tuo atveju, kai duomenys nėra pavagiami ar sunaikinami, jų modifikavimas ar neteisėtas pakeitimas gali turėti itin rimtų klinikinių pasekmių (Sametinger ir kt., 2015). Netikslūs ar pakoreguoti medicininiai duomenys gali lemti klaidingas diagnozes, netinkamą gydymą ar vaistų dozavimo klaidas. Šių incidentų pavojingumas slypi ir tame, kad jų pasekmės dažnai išryškėja tik po tam tikro laiko, kai priežastinis ryšys su kibernetiniu incidentu tampa sunkiai atsekamas (Sood ir Enbody, 2014).

Organizaciniu lygmeniu kibernetiniai incidentai dažnai atskleidžia saugumo valdymo struktūrų ir procesų brandos trūkumus. Tyrimai rodo, kad sveikatos priežiūros organizacijos, neturinčios aiškiai apibrėžtų incidentų valdymo procedūrų ir atsakomybės pasiskirstymo, chaotiškai reaguoja į incidentus ir neefektyviai priima sprendimus (Herath ir Rao, 2009). Tokios situacijos lemia antrines pasekmes, susijusias su darbuotojų perdegimu, stresu ir pasitikėjimo vadovybe mažėjimu (Bulgurcu ir kt., 2010).

Ekonominės kibernetinių incidentų pasekmės e. sveikatos sektoriuje taip pat yra reikšmingos. Tiesioginiai finansiniai nuostoliai, susiję su e. sveikatos sistemų atkūrimu, paslaugų sustabdymu ar galimomis sankcijomis, sudaro tik dalį bendro incidentų poveikio (Anderson ir kt., 2006). Netiesioginės pasekmės, tokios kaip reputacijos praradimas, pacientų pasitikėjimo sumažėjimas ir ilgalaikis veiklos neefektyvumas, dažnai turi didesnį poveikį organizacijos tvarumui ir strateginiams tikslams (Gordon ir kt., 2016, Podsakoff ir kt., 2012).

Siekiant sistemiškai apibendrinti dažniausiai e. sveikatos sistemose pasitaikančius kibernetinius incidentus, jų pobūdį ir pasekmes, toliau pateikiama 3 lentelė.

3 lentelė. Kibernetinių incidentų tipai e. sveikatos sistemose, jų apibrėžimai ir pasekmės

Incidentų tipai	Apibrėžimas	Tipinės apraiškos e. sveikatos sistemose	Pagrindinės pasekmės
Išpirkos reikalaujančios atakos (*angl. ransomware*)	Incidentai, kurių metu informacinės sistemos ar duomenys užšifruojami siekiant finansinės naudos	E. sveikatos įrašų sistemų blokavimas, IS nepasiekiamumas	Sveikatos paslaugų sustabdymas, pacientų saugos rizika
Paslaugų trikdymo atakos (*angl. DoS/DDoS*)	Atakos, kuriomis siekiama sutrikdyti sistemų prieinamumą	Registracijos sistemų, e. portalų nepasiekiamumas	Paslaugų vėlavimas, organizacinis neefektyvumas
Asmens duomenų saugumo pažeidimai	Neteisėtas konfidencialios informacijos atskleidimas	Pacientų medicininių duomenų paviešinimas	Teisinė ir reputacinė žala
Duomenų modifikavimas	Neteisėtas duomenų pakeitimas ar iškraipymas	Pakoreguoti klinikiniai duomenys	Klinikinės klaidos, ilgalaikė žala
Neautorizuota prieiga	Prieigos prie sistemų gavimas be leidimo	Vidinis ar išorinis piktnaudžiavimas	Duomenų piktnaudžiavimas
Socialinė inžinerija	Incidentai, paremti naudotojų apgaule	Sukčiavimo (*angl. Phishing*) el. laiškai, sukčiavimo skambučiai	Pradinė prieiga prie sistemų
Tiekimo grandinės incidentai	Incidentai, kylantys dėl trečiųjų šalių saugumo spragų	Informacinių technologijų tiekėjų ar paslaugų teikėjų pažeidimai	Grandininiai sistemos sutrikimai

Šaltinis: sudaryta autorės, remiantis Sametinger ir kt. (2015), Greitzer ir kt. (2014), Boyson (2014), Wirth (2019), Martin ir kt. (2017), Nacionalinio kibernetinio saugumo centro (2024) ataskaitomis

Pateikta lentelė rodo, kad e. sveikatos sistemose dažniausiai pasitaikantys kibernetiniai incidentai pasižymi nevienodu poveikio pobūdžiu, tačiau dauguma jų turi tiesioginį ar netiesioginį poveikį sveikatos paslaugų tęstinumui ir pacientų saugai. Ypač reikšmingi yra tie incidentai, kurie sutrikdo paslaugų prieinamumą arba pažeidžia klinikinių duomenų patikimumą, nes jų pasekmės dažnai peržengia organizacijos ribas ir įgyja sisteminį pobūdį.

Svarbu pažymėti, kad Nacionalinio kibernetinio saugumo centro skelbiami duomenys rodo nuoseklų kibernetinių incidentų skaičiaus augimą nacionaliniu mastu, o

didelę jų dalį sudaro socialinės inžinerijos metodais paremti incidentai. Ši tendencija atitinka tarptautiniu mastu mokslinėje literatūroje fiksuojamus procesus, susijusius su didėjančia skaitmeninių paslaugų plėtra, nuotolinio darbo modelių įsitvirtinimu ir organizacijų priklausomybe nuo informacinių sistemų (Wirth, 2019; Martin ir kt., 2017, Stoumpos ir kt., 2023). Taigi Lietuvos kibernetinio saugumo situacija e. sveikatos sektoriuje atitinka bendras tarptautines tendencijas ir patvirtina poreikį stiprinti sisteminį, brandos principais grįstą kibernetinio saugumo valdymą.

Apibendrinant 1.2. skyriuje atliktą kibernetinių grėsmių, rizikų veiksnių ir incidentų pasekmių analizę, galima teigti, kad e. sveikatos sistemų pažeidžiamumas yra nulemtas ne pavienių techninių trūkumų, bet kompleksinės technologinių, organizacinių, procesinių ir žmogiškųjų veiksnių sąveikos. E. sveikatos sistemose pasireiškiantys kibernetiniai incidentai apima platų rizikų spektrą – nuo neteisėtos prieigos, kenkimo programinės įrangos ir sistemų nepasiekiamumo iki duomenų vientisumo pažeidimų, paslaugų trikdžių ir klinikinių procesų sutrikdymo.

Atlikta analizė parodė, kad kibernetinės rizikos e. sveikatos sistemose yra glaudžiai susijusios su informacinių sistemų tarpusavio priklausomumu, technologine fragmentacija, jautrių sveikatos duomenų koncentracija, nepakankamai integruotu saugumo valdymu ir žmogiškojo veiksnio įtaka. Dėl šių veiksnių pavienės saugumo spragos gali sukelti neproporcingai didelį poveikį visai e. sveikatos ekosistemai, paveikdamos ne tik informacinių sistemų veikimą, bet ir paslaugų tęstinumą, pacientų saugą, organizacijų atsparumą, bei visuomenės pasitikėjimą e. sveikatos priežiūros paslaugomis.

Todėl veiksmingas e. sveikatos sistemų kibernetinio saugumo valdymas negali būti grindžiamas vien pavienėmis techninėmis apsaugos priemonėmis ar greitu reagavimu į įvykusius incidentus. Šiame kontekste būtinas sisteminis ir brandos principais grįstas valdymo požiūris, apimantis rizikų identifikavimą ir vertinimą, prevencinių priemonių planavimą, koordinuotą reagavimą, atsakomybių paskirstymą, incidentų pasekmių analizę ir organizacinį mokymąsi. Toks požiūris sudaro pagrindą pereiti prie integruotų informacijos saugumo valdymo sistemų, tarptautinių standartų ir kibernetinio saugumo brandos modelių analizės, kuri toliau plėtojama 1.3 skyriuje.

1.3. Informacijos saugumo valdymo sistemos

Ankstesniame skyriuje atlikta kibernetinių grėsmių, rizikų veiksnių ir incidentų pasekmių analizė parodė, kad e. sveikatos sistemų pažeidžiamumą lemia ne tik pavieniai techniniai trūkumai, bet ir sisteminės organizacinės, procesinės bei žmogiškojo veiksnio nulemtos spragos. Dėl šios priežasties e. sveikatos sistemų kibernetinis saugumas negali būti užtikrinamas fragmentiškai, taikant tik atskiras technines apsaugos priemones. Reikalingas nuoseklus, struktūruotas ir organizacijos valdymo procesus apimantis požiūris, leidžiantis kibernetinį saugumą integruoti į bendrą institucijos veiklos, rizikų valdymo ir paslaugų tęstinumo užtikrinimo sistemą.

Šiame kontekste informacijos saugumo valdymo sistemos įgyja ypatingą reikšmę. Jos suprantamos kaip formalizuotų politikų, procedūrų, procesų, atsakomybių ir kontrolės priemonių visuma, skirta informacijos konfidencialumui, vientisumui ir

prieinamumui užtikrinti. Skirtingai nei pavienės techninės saugumo priemonės, informacijos saugumo valdymo sistemos sudaro prielaidas saugumą valdyti sistemiškai, identifikuoti ir vertinti rizikas, planuoti prevencines priemones, apibrėžti atsakomybes, stebėti saugumo būklę ir nuosekliai didinti organizacijos saugumo brandą.

Tarptautinėje praktikoje informacijos saugumo valdymo sistemos dažniausiai grindžiamos standartizuotais modeliais, gairėmis ir brandos vertinimo priemonėmis. Tokie standartai ir modeliai leidžia užtikrinti nuoseklų saugumo valdymo procesų kūrimą, palyginamą organizacijų saugumo lygio vertinimą ir sistemingą tobulinimą. Jie apima ne tik techninių kontrolės priemonių taikymą, bet ir vadovybės atsakomybę, rizikų valdymą, incidentų valdymą, atitiktį teisės aktams, veiklos tęstinumą bei nuolatinio tobulinimo principus.

E. sveikatos sistemų kontekste šių sistemų reikšmė dar labiau sustiprėja dėl tvarkomų asmens sveikatos duomenų jautrumo, informacinių sistemų tarpusavio priklausomumo, paslaugų tęstinumo svarbos ir griežto reguliacinio režimo. Kibernetinio saugumo pažeidimai šiame sektoriuje gali sukelti ne tik technologinių ar ekonominių, bet ir tiesioginių klinikinių, organizacinių bei reputacinių pasekmių. Todėl informacijos saugumo valdymo sistemos laikytinos būtinu pagrindu, leidžiančiu e. sveikatos organizacijoms pereiti nuo reaktyvaus incidentų valdymo prie prevencinio, rizikomis grįsto ir brandos principais paremto saugumo valdymo.

Atsižvelgiant į tai, tolesniuose šio skyriaus poskyriuose analizuojamos pagrindinės informacijos saugumo valdymo sistemos, standartai ir brandos vertinimo modeliai, reikšmingi e. sveikatos sistemų kibernetinio saugumo valdymui. Pirmiausia nagrinėjami ISO/IEC standartai, apibrėžiantys informacijos saugumo valdymo sistemos struktūrą, rizikų vertinimo ir kontrolės priemonių taikymo principus. Vėliau aptariami Europos Sąjungos reguliaciniai instrumentai, ypač TIS2 direktyva, darantys tiesioginę įtaką sveikatos sektoriaus kibernetinio saugumo valdymui. Galiausiai analizuojami kibernetinio saugumo brandos modeliai, leidžiantys vertinti organizacijų pasirengimą, valdymo procesų nuoseklumą ir atsparumo kibernetinėms grėsmėms didinimo prielaidas.

1.3.1. ISO/IEC 27001, 27005 ir susiję standartai

Informacijos saugumo valdymo sistemos (ISVS) yra vienas iš pagrindinių organizacinio kibernetinio saugumo užtikrinimo mechanizmų, ypač sektoriuose, kuriuose tvarkomi didelės apimties jautrūs duomenys ir nuo informacinių sistemų patikimumo tiesiogiai priklauso paslaugų teikimo tęstinumas. E. sveikatos sistemose informacijos saugumo valdymas negali būti orientuotas vien į techninių kontrolės priemonių taikymą, kadangi tokiose sistemose saugumo sprendimai glaudžiai susiję su klinikiniais procesais. Dėl šios priežasties mokslinėje literatūroje pabrėžiama būtinybė taikyti sisteminius, tarptautiniais standartais grįstus informacijos saugumo valdymo modelius, kurie užtikrintų nuoseklų ir integruotą kibernetinio saugumo valdymą.

ISO/IEC 27001 standartas yra laikomas kertiniu informacijos saugumo valdymo sistemos kūrimo ir palaikymo dokumentu. Naujausia šio standarto redakcija

akcentuoja rizikomis grįstą požiūrį, kai saugumas suvokiamas kaip nuolat veikianti vadybinė sistema, integruota į organizacijos strateginį valdymą. Tyrimai rodo, kad ISO/IEC 27001 diegimas skatina organizacijas formaliai apibrėžti saugumo tikslus, atsakomybes ir sprendimų priėmimo procesus, taip didinant organizacinį atsparumą kibernetinėms grėsmėms (von Solms ir von Solms, 2018; Culot ir kt., 2021, Disterer, 2013). E. sveikatos įstaigose tai ypač svarbu, nes saugumo sprendimai turi būti suderinti su pacientų saugos, paslaugų prieinamumo ir veiklos tęstinumo reikalavimais.

ISO/IEC 27001 metodologinis pagrindas remiasi nuolatinio tobulinimo ciklu (angl. *Plan Do Check Act*), kuris leidžia organizacijoms sistemingai planuoti saugumo priemones, jas įgyvendinti, vertinti jų veiksmingumą ir koreguoti atsižvelgiant į besikeičiančią grėsmių aplinką. Mokslinėje literatūroje pabrėžiama, kad toks požiūris leidžia pereiti nuo reaktyvaus saugumo valdymo prie proaktyvios, prevencijos principais grįstos praktikos (Aven, 2016; Podrecca ir kt., 2025).

ISO/IEC 27005 standartas papildo ISO/IEC 27001, pateikdamas struktūruotą informacijos saugumo rizikų valdymo metodiką. Jame rizika apibrėžiama kaip grėsmių, pažeidžiamumų ir galimo poveikio sąveikos rezultatas. Tyrimai pabrėžia, kad e. sveikatos sistemose rizikų vertinimas turi apimti ne tik techninius, bet ir organizacinius bei žmogiškuosius veiksnius, nes būtent jų sąveika dažnai lemia incidentų mastą ir pasekmes (Appari ir Johnson, 2010; Suorsa, 2024). ISO/IEC 27005 leidžia sistemingai identifikuoti ir vertinti šias rizikas bei pasirinkti proporcingas rizikų mažinimo priemones.

Svarbų vaidmenį praktiniame saugumo valdyme atlieka ISO/IEC 27002 standartas, kuris pateikia išsamų saugumo kontrolės priemonių rinkinį. Šis standartas padeda organizacijoms įgyvendinti ISO/IEC 27001 reikalavimus, apibrėždamas konkrečias prieigos kontrolės priemones, incidentų valdymo, tiekėjų valdymo ir kitose srityse. Tyrimai rodo, kad sveikatos sektoriuje ISO/IEC 27002 taikymas leidžia geriau suderinti technologinius sprendimus su organizaciniais procesais (Kwon ir Johnson, 2014; McLeod ir Dolezel, 2018).

Incidentų valdymo aspektą detalizuoja ISO/IEC 27035 standartų šeima, kuri apima pasirengimą incidentams, reagavimą ir organizacinį mokymąsi po incidentų. Mokslinėje literatūroje pabrėžiama, kad struktūruotas incidentų valdymas yra būtina sąlyga siekiant sumažinti incidentų poveikį ir užtikrinti paslaugų tęstinumą (Ransbotham ir kt., 2012; Gordon ir kt., 2017). E. sveikatos sistemose tai ypač aktualu dėl tiesioginės sąsajos su pacientų sauga.

Apibendrinant galima teigti, kad ISO/IEC 27001, ISO/IEC 27005 ir susiję standartai sudaro nuoseklią informacijos saugumo valdymo sistemą, leidžiančią integruoti kibernetinį saugumą į bendrą organizacijos valdymo struktūrą. Moksliniai tyrimai patvirtina, kad šių standartų taikymas padeda pereiti nuo fragmentuotų techninių sprendimų prie brandos principais grįsto, sisteminio saugumo valdymo.

1.3.2. TIS2 direktyva ir jos įgyvendinimas

Per pastarąjį dešimtmetį Europos Sąjungos kibernetinio saugumo politika transformavosi iš sektorinėmis rekomendacijomis ir minimaliais atitikties reikalavimais grindžiamo reguliavimo į nuoseklesnę, rizikomis grįstą reguliacinę sistemą. Šio poslinkio branduoliu tapo Tinklų ir informacinių sistemų saugumo direktyva (TIS2, angl. *NIS2 Directive*), kuria siekiama suvienodinti kibernetinio saugumo lygį visoje Europos Sąjungoje, išplečiant taikymo sritį ir sugriežtinant valdymo, pranešimą apie incidentus bei priežiūros mechanizmus (Europos Parlamentas ir Taryba, 2022). Sveikatos sektorius yra traktuojamas kaip vienas kritiškiausių dėl paslaugų tęstinumo svarbos ir tvarkomų duomenų jautrumo, todėl TIS2 įtvirtina prielaidas kibernetinį saugumą vertinti ne kaip „IT uždavinį", o kaip strateginio valdymo sritį.

Svarbi TIS2 direktyvos ypatybė – rizikų valdymo priemonių formalizavimas ir jų sujungimas su organizacine atsakomybe. Direktyva reikalauja, kad saugumo priemonės būtų taikomos sistemiškai, apimtų prevenciją, aptikimą, reagavimą ir atkūrimą, o jų parinkimas būtų siejamas su organizacijos rizikų profiliu, veiklos kritiškumu ir galimo poveikio mastu (Europos Parlamentas ir Taryba, 2022). Ši logika tiesiogiai dera su disertacijos tema, nes kibernetinio saugumo valdymo modelio vertinimas e. sveikatos sistemai iš esmės remiasi tuo, ar organizacija turi mechanizmus ne tik „apsaugoti", bet ir valdyti rizikas kaip nuolatinį ciklą.

Lietuvos kontekste TIS2 įgyvendinimas yra aiškiai susietas su nacionaliniais valdymo instrumentais, kuriuos koordinuoja Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (NKSC). NKSC pateikia praktiškai orientuotą įgyvendinimo logiką: subjektų identifikavimą, jų priskyrimą kategorijoms (esminiai ir svarbūs), įtraukimą į Kibernetinio saugumo subjektų registrą, Kibernetinio saugumo informacinę sistemą (KSIS) bei reikalavimų įgyvendinimą pagal pereinamuosius terminus (NKSC, 2024).

NKSC pabrėžiama, kad įstatymo įgyvendinimas numato aiškius etapus ir pereinamuosius laikotarpius. Pirma, vyksta subjektų identifikavimas ir įtraukimas į registrą; antra, organizacijos, gavusios patvirtinimą, turi prisijungti prie KSIS ir pateikti informaciją apie veiklą bei paslaugas; trečia, reikalavimai pradedami taikyti per pereinamąjį laikotarpį – organizaciniams reikalavimams skiriant 12 mėn., techniniams – 24 mėn. nuo įtraukimo į registrą (NKSC, 2024). Praktinėje plotmėje tai reiškia, kad valdymo modelis negali apsiriboti vien „galutine atitiktimi", bet turi apimti ir įgyvendinimo trajektoriją (t. y. kaip organizacija pereina nuo esamos būklės prie reikalaujamo saugumo lygio).

Be pereinamųjų terminų, NKSC aiškiai akcentuoja ir valdymo struktūros reikalavimus. Pavyzdžiui, organizacijos turi užtikrinti saugumo funkcijų nepriklausomumą nuo kasdienio informacinių technologijų administravimo. NKSC nurodo, kad kibernetinio saugumo vadovas (CISO) negali vykdyti funkcijų, susijusių su tinklų ar informacinių sistemų administravimu, ir taip įtvirtina kontrolės funkcijos atskyrimą nuo vykdomųjų (operacinių) veiklų (NKSC, 2024). E. sveikatos sektoriuje tai ypač aktualu dėl istorinio modelio, kai saugumas kartais sutapatinamas su infrastruktūros

priežiūra, o ne su rizikų valdymu.

Kitas reikšmingas TIS2 ir nacionalinio įgyvendinimo aspektas – tiekimo grandinės saugumas. NKSC išskiria, kad dirbant su paslaugų teikėjais būtina taikyti tiekimo grandinės reikalavimus, į sutartis įtraukti konkrečius saugumo punktus, apibrėžti trečiųjų šalių prieigos lygius, taikyti žemiausios privilegijos principą, užtikrinti duomenų grąžinimą arba sunaikinimą paslaugų pabaigoje bei fiksuoti užbaigimo veiksmus (NKSC, 2024). E. sveikatos sistemų ekosistemoje, kur būdingi daugialypiai tiekėjai (programinės įrangos gamintojai, debesijos paslaugos, medicininių įrenginių tiekėjai), ši dimensija tampa viena svarbiausių vertinant realią saugumo brandą.

Galiausiai, NKSC pabrėžia, kad valdymo sistemoje turi atsirasti ir reguliarus vertinimas. Organizacijos periodiškai (ne rečiau kaip kartą per 3 metus), turi atlikti kibernetinio saugumo auditą, taip pat valdyti incidentus, užtikrinti veiklos tęstinumą ir organizuoti mokymus (NKSC, 2024). Kibernetinio saugumo kompetencijų stiprinimui gali būti pasitelkiamos pažangios mokymosi technologijos, tokios kaip dirbtinis intelektas, pokalbių robotai ir robotizuotos sistemos, nes jos sudaro sąlygas individualizuotam mokymuisi, grįžtamajam ryšiui ir interaktyvioms mokymosi patirtims (Limba ir kt., 2024). Šie elementai tiesiogiai siejasi su kibernetinio saugumo valdymo modelio vertinimo logika, brandus modelis turi turėti ne tik politiką, bet ir tikrinamus įrodymus (auditą, rodiklius, mokymų sistemą, tęstinumo planus).

Atsižvelgiant į tai, TIS2 direktyvą tikslinga vertinti kaip reguliacinį mechanizmą, kuris sujungia tris lygmenis: (1) ES normatyvinius reikalavimus, (2) nacionalinę įgyvendinimo infrastruktūrą (registrai, KSIS, metodikos) ir (3) organizacinį valdymo brandos turinį (politikos, rizikų valdymas, tiekimo grandinė, auditai, reagavimas, tęstinumas).

Tarptautiniu mastu TIS2 kryptis atspindi bendrą poslinkį nuo „atitikties dokumentams“ prie atsparumo ir valdymo brandos. Valstybės siekia, kad kritiniai sektoriai turėtų aiškius incidentų valdymo, tęstinumo ir tiekimo grandinės kontrolės mechanizmus, o atsakomybė būtų priskirta valdymo grandinei, o ne vien IT padaliniams (Europos Parlamentas ir Taryba, 2022). Lietuvos atvejis šią tendenciją konkretina per NKSC kuriamą įgyvendinimo infrastruktūrą: registrą, KSIS, pereinamuosius terminus, kurie sudaro sąlygas saugumą vertinti pagal įrodymus (procesus, dokumentus, auditus, sutartis), o ne vien deklaracijas (NKSC, 2024). Dėl to Lietuvos praktika yra tinkama bazė empiriniam vertinimui disertacijoje, nes leidžia operaciniu lygmeniu pamatuoti, kaip direktyvos reikalavimai virsta organizaciniais sprendimais e. sveikatos ekosistemoje.

4 lentelė. TIS2 (*angl. NIS2*) direktyvos reikalavimų suvedimas į kibernetinio saugumo valdymo modelio dimensijas

Valdymo dimensija	TIS2 reikalavimų kryptis	Pagrindinis turinys e. sveikatos sistemos kontekste	Galimi vertinimo indikatoriai (empirikai)
Strateginis valdymas	Vadovybės atsakomybė ir įsitraukimas	Aukščiausio lygmens vadovybė atsakinga už kibernetinio saugumo politiką, sprendimų priėmimą ir išteklių paskirstymą; saugumas integruojamas į organizacijos strategiją	Patvirtinta kibernetinio saugumo strategija; vadovybės dalyvavimas sprendimuose; saugumo klausimų įtraukimas į strateginius dokumentus
Valdymo struktūra	Funkcijų ir atsakomybių apibrėžimas	Aiškiai apibrėžtos kibernetinio saugumo funkcijos; kibernetinio saugumo vadovo (CISO) nepriklausomumas nuo IT administravimo funkcijų	CISO paskyrimas; funkcijų atskyrimas; atsakomybių dokumentavimas
Rizikų valdymas	Sisteminis rizikų vertinimas	Reguliarus kibernetinių rizikų identifikavimas, vertinimas ir valdymas, atsižvelgiant į e. sveikatos paslaugų kritiškumą	Rizikų vertinimo periodiškumas; taikoma metodika; rizikų registras
Incidentų valdymas	Incidentų aptikimas, reagavimas ir pranešimas	Nustatytos procedūros incidentams identifikuoti, valdyti ir pranešti kompetentingoms institucijoms per nustatytus terminus	Incidentų valdymo planas; pranešimų savalaikiškumas; atliktos pratybos
Veiklos tęstinumas	Atsparumo ir atkūrimo užtikrinimas	Priemonės užtikrinti kritinių e. sveikatos paslaugų tęstinumą incidentų metu ir po jų	Atsarginės kopijos; atkūrimo laikas; tęstinumo planai
Tiekimo grandinės saugumas	Trečiųjų šalių rizikų valdymas	Kibernetinio saugumo reikalavimai tiekėjams, ypač programinės įrangos ir paslaugų teikėjams	Tiekėjų vertinimo kriterijai; sutartiniai saugumo reikalavimai; auditai
Atitiktis ir auditai	Kontrolė ir priežiūra	Atitikties TIS2 reikalavimams stebėsena, vidaus ir išorės auditai	Atliktų auditų skaičius; nustatytos neatitiktys; korekciniai veiksmai
Žmogiškieji ištekliai	Kompetencijų ir sąmoningumo stiprinimas	Darbuotojų mokymai, sąmoningumo didinimas, socialinės inžinerijos rizikų mažinimas	Mokymų reguliarumas; dalyvių skaičius; testavimo rezultatai

Šaltinis: sudaryta autorės, remiantis Direktyva (ES) 2022/2555 (Europos Parlamentas ir Taryba, 2022) ir Nacionalinio kibernetinio saugumo centro informacija apie TIS2 įgyvendinimą Lietuvoje (NKSC, 2024)

Ši lentelė atskleidžia, kad TIS2 direktyvos reikalavimai nėra vien techninio pobūdžio, bet apima visą kibernetinio saugumo valdymo ciklą – nuo strateginio planavimo ir organizacinės struktūros iki rizikų, incidentų, tiekimo grandinės ir veiklos tęstinumo valdymo. Tokia reikalavimų struktūra parodo, jog kibernetinis saugumas e. sveikatos sistemose turi būti vertinamas kaip kompleksinis valdymo reiškinys, o ne izoliuotų technologinių priemonių visuma.

Svarbu pažymėti, kad kiekvienai identifikuotai valdymo dimensijai galima priskirti aiškius vertinimo indikatorius, kurie sudaro prielaidas empiriniam kibernetinio saugumo valdymo brandos vertinimui. Tai leidžia TIS2 reikalavimus tiesiogiai integruoti į disertacijoje kuriamą kibernetinio saugumo valdymo modelį ir vėlesniuose skyriuose naudoti juos kaip struktūrinį pagrindą kokybinei analizei.

1.3.3. Kibernetinio saugumo brandos modeliai

Mokslinėje literatūroje pabrėžiama, kad kibernetinio saugumo būklės vertinimas, apsiribojantis pavienių techninių priemonių ar formalaus atitikties reikalavimams tikrinimu, neleidžia visapusiškai įvertinti organizacijos gebėjimo atsispirti kibernetinėms grėsmėms. Ilgalaikis saugumas priklauso nuo to, kaip nuosekliai organizacijoje valdomi saugumo procesai, kaip jie integruojami į bendrą valdymo sistemą ir kaip sistemingai tobulinami atsižvelgiant į kintančią grėsmių aplinką (Siponen ir kt., 2014; Tondel ir kt., 2014, Scheibner ir kt., 2021, Ksibi ir kt., 2022).

Šiame kontekste kibernetinio saugumo brandos modeliai laikytini svarbia analitine priemone, leidžiančia įvertinti ne tik esamą saugumo būklę, bet ir organizacijos raidos kryptį. Brandos modelių logika grindžiama prielaida, kad saugumo valdymas vystosi palaipsniui – nuo fragmentuotų, nestruktūruotų ir reaktyvių sprendimų iki formaliai apibrėžtų, valdomų, matuojamų ir nuolat tobulinamų procesų. Toks požiūris leidžia kibernetinį saugumą vertinti kaip ilgalaikį organizacinį gebėjimą, o ne kaip vienkartinę technologinę intervenciją.

Vienu ankstyviausių brandos koncepcijos taikymo pavyzdžių laikomas gebėjimų brandos modelis (angl. Capability Maturity Model, CMM), iš pradžių sukurtas programinės įrangos kūrimo procesams vertinti. Nors šis modelis nebuvo skirtas kibernetinio saugumo sričiai, jo pagrindinė logika – procesų formalizavimas, standartizavimas, vertinimas ir nuoseklus tobulinimas – tapo svarbiu pagrindu vėlesniems saugumo brandos modeliams. Mokslinėje literatūroje pažymima, kad aukštesnis procesų brandos lygis paprastai siejamas su didesniu organizacijos gebėjimu sistemiškai identifikuoti grėsmes, valdyti rizikas ir nuosekliau reaguoti į saugumo incidentus.

Informacinių technologijų valdymo srityje plačiai taikomas COBIT modelis, kuris moksliniuose tyrimuose vertinamas kaip priemonė, padedanti suderinti informacinių technologijų valdymą su organizacijos strateginiais tikslais (De Haes ir Van Grembergen, 2015). Kibernetinio saugumo požiūriu COBIT reikšmingas tuo, kad saugumo kontrolės priemonės šiame modelyje siejamos su rizikų valdymu, atsakomybių paskirstymu, veiklos kontrole ir valdymo skaidrumu. Todėl jo taikymas gali sustiprinti vadovybės įsitraukimą į saugumo sprendimus, pagerinti vidinės kontrolės

mechanizmus ir padėti sistemingiau valdyti kibernetinio saugumo procesus.

Vis dėlto COBIT taikymas sveikatos sektoriuje turi ir tam tikrų ribotumų. Literatūroje pažymima, kad šis modelis pasižymi aukštu formalizavimo lygiu ir reikalauja reikšmingų organizacinių, žmogiškųjų bei laiko išteklių. Dėl šios priežasties jo taikymas gali būti sudėtingas sveikatos priežiūros organizacijose, kurios veikia intensyviomis kasdienės veiklos sąlygomis, turi ribotus išteklius ir privalo derinti saugumo reikalavimus su nepertraukiamu sveikatos priežiūros paslaugų teikimu (De Haes ir Van Grembergen, 2015, ISACA, 2019).

Pastarąjį dešimtmetį daug dėmesio skiriama rizikomis grįstam požiūriui, įtvirtintam Nacionalinio standartų ir technologijų instituto kibernetinio saugumo pagrindų struktūroje (angl. NIST Cybersecurity Framework). Moksliniuose tyrimuose pabrėžiama, kad ši struktūra sudaro prielaidas lanksčiai pritaikyti saugumo priemones skirtingoms organizacinėms aplinkoms, išlaikant nuoseklią valdymo logiką per pagrindines funkcijas: identifikavimą, apsaugą, aptikimą, reagavimą ir atkūrimą (Bodeau ir Graubart, 2017). Šis modelis ypač reikšmingas sudėtingoms, tarpinstitucinėms sistemoms, kuriose būtina derinti skirtingų suinteresuotųjų šalių atsakomybes ir valdymo interesus (Linkov ir kt., 2018).

ISO standartais grindžiami brandos vertinimo požiūriai mokslinėje literatūroje dažnai siejami su informacijos saugumo valdymo sistemų nuoseklumu ir metodiniu stabilumu. Tokie modeliai sudaro prielaidas sistemiškai valdyti saugumo procesus ir užtikrinti jų suderinamumą su kitomis organizacijos valdymo sistemomis (Da Veiga ir Eloff, 2007; Ključnikov ir kt., 2019). Tačiau kartu pažymima, kad ISO pagrindu formuojami vertinimo mechanizmai dažnai labiau orientuoti į atitikties užtikrinimą nei į dinamišką saugumo gebėjimų vystymą. Todėl sparčiai kintančioje kibernetinių grėsmių aplinkoje jų taikymą būtina papildyti rizikų, incidentų, atsparumo ir organizacinio mokymosi dimensijomis.

E. sveikatos sistemų kontekste brandos modelių taikymas turi būti vertinamas kritiškai. Sveikatos sektoriui būdingas socio-techninis kompleksiškumas, griežtas reguliavimas, jautrių asmens sveikatos duomenų tvarkymas, informacinių sistemų tarpusavio priklausomybė ir tiesioginis ryšys su pacientų sauga. Todėl bendrieji brandos modeliai negali būti mechaniškai perkeliami į e. sveikatos aplinką. Jie turi būti adaptuojami atsižvelgiant į konkrečius e. sveikatos sistemos komponentus: nacionalinę infrastruktūrą, sveikatos priežiūros įstaigų informacines sistemas, pacientų prieigos kanalus, e. recepto ir registracijos posistemes, duomenų mainų mechanizmus, medicininius įrenginius bei veiklos tęstinumo procesus.

Šiame disertaciniame tyrime tarptautiniai standartai, teisinio reguliavimo sistemos, ENISA gairės ir brandos modeliai vertinami ne kaip atskiros ar konkuruojančios priemonės, bet kaip tarpusavyje susijęs normatyvinis ir metodinis pagrindas. Jų reikšmė kuriamam kibernetinio saugumo valdymo modeliui atsiskleidžia tik tada, kai šie šaltiniai susiejami su e. sveikatos sistemos architektūra, duomenų srautais, rizikos taškais ir organizacinėmis atsakomybėmis. Ši sąsaja apibendrinama 5 lentelėje.

5 lentelė. Kibernetinio saugumo valdymo modelio teorinių ir normatyvinių šaltinių reikšmė bei ribotumai e. sveikatos sistemos kontekste

Šaltinių grupė	Pagrindinė reikšmė kuriamam modeliui	Ribotumas e. sveikatos sistemos kontekste
ISO/IEC informacijos saugumo standartai	Pagrindžia rizikų valdymo, kontrolės priemonių, ISMS, nuolatinio tobulinimo ir atsakomybės principus	Nepateikia e. sveikatos sistemos architektūrai specifinio valdymo modelio
TIS2 reikalavimai	Pabrėžia kritinių sektorių atsparumą, incidentų valdymą, tiekimo grandinių saugumą ir vadovybės atsakomybę	Labiau apibrėžia atitikties prievoles, o ne praktinę e. sveikatos sistemos valdymo struktūrą
ENISA gairės	Padeda identifikuoti sektoriaus rizikas, grėsmes, incidentų valdymo ir atsparumo stiprinimo kryptis	Daugiau orientuotos į bendrą kibernetinio saugumo praktiką, todėl turi būti adaptuojamos konkrečiai e. sveikatos ekosistemai
Brandos modeliai	Leidžia vertinti organizacijos gebėjimų lygį, procesų institucionalizavimą ir tobulinimo kryptis	Brandos lygiai turi būti susieti su konkrečiais e. sveikatos komponentais, o ne taikomi abstrakčiai

Šaltinis: sudaryta autorės

Apibendrinant galima teigti, kad kibernetinio saugumo brandos modeliai yra reikšmingi saugumo valdymo vertinimui, tačiau jų taikymas e. sveikatos sistemoje reikalauja kryptingo pritaikymo. Jų vertė atsiskleidžia ne pavienių saugumo priemonių vertinime, bet gebėjime sistemiškai įvertinti organizacijos pasirengimą ilgalaikėje perspektyvoje valdyti kibernetines rizikas, identifikuoti silpnąsias vietas ir planuoti tobulinimo kryptis. Kartu tarptautiniai standartai, TIS2 reikalavimai, ENISA gairės ir brandos modeliai sudaro tik pradinį kibernetinio saugumo valdymo pagrindą. Jie apibrėžia bendruosius principus, tačiau neatsako į klausimą, kaip šie principai turėtų būti suderinti su konkrečia e. sveikatos sistemos struktūra, klinikiniais ir administraciniais procesais, tarpinstituciniais duomenų mainais, naudotojų vaidmenų įvairove, medicininių įrenginių saugumu ir paslaugų tęstinumo poreikiais.

Todėl šiame darbe šie šaltiniai naudojami kaip normatyvinis ir metodinis modelio kūrimo pagrindas, kuris leidžia pereiti nuo bendrųjų informacijos saugumo valdymo sistemų analizės prie konkretaus sveikatos sektoriaus kibernetinio saugumo valdymo ypatumų. Todėl kitame disertacijos skyriuje dėmesys sutelkiamas į e. sveikatos sistemų struktūrą, informacinių sistemų sąveiką, asmens sveikatos duomenų apsaugą ir konfidencialumo užtikrinimo aspektus.

1.4. Kibernetinio saugumo valdymas sveikatos sektoriuje

Kibernetinio saugumo valdymas sveikatos sektoriuje turi būti analizuojamas

pirmiausia per e. sveikatos sistemos struktūrą, nes būtent sistemos architektūra lemia, kur atsiranda kritiniai duomenų srautai, prieigos taškai, atsakomybių ribos ir galimos kibernetinio pažeidžiamumo zonos. E. sveikatos sistema nėra vien informacinė platforma ar pavienių skaitmeninių paslaugų rinkinys. Tai daugiasluoksnė socio-techninė ekosistema, kurioje sąveikauja nacionalinė sveikatos informacinė infrastruktūra, sveikatos priežiūros įstaigų informacinės sistemos, laboratorijų ir diagnostikos sistemos, e. recepto, registracijos ir pacientų portalų posistemės, sveikatos specialistai, pacientai, administratoriai, politikos formuotojai, paslaugų teikėjai ir technologiniai tiekėjai (Ewoh ir Vartiainen, 2024; Ewoh ir Vartiainen, 2025).

Naujausi sveikatos informacinių sistemų architektūros tyrimai pabrėžia, kad skaitmeninės sveikatos ekosistemos dažnai išlieka fragmentuotos, sudarytos iš izoliuotų programinių sprendimų, o tai apsunkina sąveikumą, duomenų kokybės užtikrinimą, atsakomybių paskirstymą ir kibernetinio saugumo kontrolę (Casanova, Villa-Garzon ir Branch-Bedoya, 2025). Sisteminiu požiūriu e. sveikatos kibernetinis saugumas priklauso ne tik nuo atskirų apsaugos priemonių, bet ir nuo to, kaip saugiai organizuojamas duomenų judėjimas tarp sistemos komponentų, kaip apibrėžiami naudotojų vaidmenys, kaip valdomos sąsajos su išoriniais tiekėjais ir kaip užtikrinamas paslaugų tęstinumas incidento atveju (Pavao, Bastardo ir Rocha, 2024).

Todėl šiame darbe e. sveikatos sistema analizuojama kaip kompleksinis valdymo objektas, kuriam būtinas ne tik techninis, bet ir organizacinis bei procesinis kibernetinio saugumo modeliavimas. Toks požiūris leidžia pereiti nuo deklaratyvaus saugumo principų išvardijimo prie kritinės analizės, kokios konkrečios e. sveikatos sistemos savybės lemia kibernetinio saugumo valdymo poreikį ir kokios modelio dimensijos turi būti įtrauktos siekiant didinti sistemos atsparumą.

Sveikatos sektorius pastaraisiais dešimtmečiais patiria intensyvią skaitmeninę transformaciją, kuri iš esmės keičia sveikatos paslaugų organizavimo, klinikinių sprendimų priėmimo ir duomenų valdymo praktiką. E. sveikatos įrašų, integruotų klinikinių informacinių sistemų, nuotolinių paslaugų bei medicininių prietaisų interneto sprendimų plėtra sudaro prielaidas didesniam paslaugų prieinamumui ir efektyvumui, tačiau kartu ženkliai padidina kibernetinių grėsmių poveikį sveikatos priežiūros infrastruktūrai (Kruse ir kt., 2017; Jalali ir Kaiser, 2018).

Kibernetinio saugumo valdymas sveikatos sektoriuje turi būti analizuojamas ne tik kaip informacinių sistemų apsaugos klausimas, bet ir kaip tiesiogiai su pacientų sauga, paslaugų tęstinumu ir visuomenės pasitikėjimu susijęs vadybinis reiškinys. Naujausi tyrimai rodo, kad sveikatos priežiūros organizacijos susiduria su kompleksiniu grėsmių spektru, apimančiu Išpirkos reikalaujančias (angl. *ransomware*) atakas, duomenų nutekėjimą, neautorizuotą prieigą, tiekimo grandinės pažeidžiamumus, trečiųjų šalių rizikas, medicininių įrenginių saugumo spragas ir žmogiškojo veiksnio nulemtus incidentus (Qureshi ir Koo, 2026; Rogge ir Bohnet-Joschko, 2026; Cornejo, 2026; Brantly, 2026; Clarke ir Martin, 2024). Dėl to e. sveikatos sistemos kibernetinis saugumas negali būti vertinamas vien per techninių kontrolės priemonių prizmę, būtina įtraukti organizacinį, procesinį, technologinį ir klinikinį saugumo aspektus.

Kritiniu požiūriu sveikatos sektoriaus kibernetinis pažeidžiamumas kyla iš to, kad

skaitmeninės sveikatos technologijos tampa integruota kasdienio klinikinio darbo dalimi. Kibernetinis incidentas gali paveikti ne tik duomenų konfidencialumą, bet ir gydymo sprendimų kokybę, pacientų registraciją, diagnostinių duomenų prieinamumą, e. receptų veikimą bei sveikatos priežiūros paslaugų tęstinumą (Aldosari, 2025; Alanazi, 2023; Kissi ir kt., 2024, Markopoulou ir kt., 2021). Todėl kibernetinis saugumas suprantamas kaip e. sveikatos sistemos patikimumo ir veiklos tęstinumo sąlyga, o ne kaip izoliuotas informacinių technologijų padalinio atsakomybės laukas.

Šiame kontekste kibernetinis saugumas sveikatos sektoriuje tampa ne tik informacinių sistemų apsaugos, bet ir pacientų saugos bei paslaugų tęstinumo užtikrinimo klausimu.

Kritinės infrastruktūros kibernetinio saugumo valdymas reikalauja ne tik techninių kontrolės priemonių, bet ir nuoseklios saugumo politikos, kurioje būtų įvertinti veikimo režimai, būtinas apsaugos lygis, atsakomybių paskirstymas ir jautrių sektorių apsaugos poreikiai (Tvaronavičienė ir kt., 2022). Mokslinėje literatūroje pabrėžiama, kad kibernetinio saugumo valdymas sveikatos sektoriuje pasižymi specifiniais bruožais, išskiriančiais jį iš kitų kritinės infrastruktūros sričių. Sveikatos organizacijos veikia itin sudėtingoje aplinkoje, kurioje būtina suderinti aukštus informacijos prieinamumo reikalavimus su griežtais konfidencialumo ir vientisumo standartais (Appari ir Johnson, 2010; McLeod ir Dolezel, 2018). Skirtingai nei daugelyje kitų sektorių, sveikatos priežiūros įstaigose informacinių sistemų sutrikimai gali turėti tiesioginių pasekmių pacientų gyvybei ir sveikatai, todėl rizikos tolerancija čia yra itin ribota (Coiera ir kt., 2012).

Kibernetinio saugumo valdymo problematiką sveikatos sektoriuje apsunkina ir organizaciniai veiksniai. Tyrimai rodo, kad sveikatos priežiūros organizacijose saugumo valdymas dažnai fragmentuojamas tarp skirtingų padalinių, o atsakomybės už kibernetinį saugumą nėra aiškiai apibrėžtos (Kellermann ir Jones, 2013; Ransbotham ir kt., 2012). Be to, riboti finansiniai ištekliai dažnai lemia tai, kad saugumo priemonės suvokiamos kaip papildoma administracinė našta, o ne integrali organizacijos valdymo dalis (Ashenden ir Lawrence, 2016).

Pastaraisiais metais vis daugiau tyrimų pabrėžia, kad efektyvus kibernetinio saugumo valdymas sveikatos sektoriuje turi būti grindžiamas sisteminiu ir brandos principais paremtu požiūriu. Tai reiškia perėjimą prie proaktyvaus rizikų identifikavimo, nuolatinio saugumo gebėjimų stiprinimo ir organizacinio mokymosi (Bohme ir kt., 2021; Suorsa, 2024). Tokį požiūrį ypač skatina didėjantis tarpinstitucinis ir tarpsektorinis duomenų mainų mastas, kuris lemia, kad pavienės organizacijos saugumo spragos gali turėti sisteminį poveikį visai sveikatos ekosistemai (Radanliev ir kt., 2019).

Atsižvelgiant į šias aplinkybes, kibernetinio saugumo valdymas sveikatos sektoriuje turi būti analizuojamas kaip kompleksinis valdymo procesas, apimantis strateginius sprendimus, organizacines struktūras, procesų sąveiką ir žmogiškuosius veiksnius. Tolesniuose šio skyriaus poskyriuose detaliau nagrinėjama e. sveikatos sistemų struktūra ir veikimo principai, informacinių sistemų integracijos ir sąveikos problematika bei asmens sveikatos duomenų apsaugos ir konfidencialumo užtikrinimo ypatumai, kurie sudaro esminį pagrindą kibernetinio saugumo valdymo modelio tikslinimui.

1.4.1. E. sveikatos sistemos struktūra ir veikimo principai

E. sveikatos sistema paprastai suprantama ne kaip viena informacinė sistema, o kaip tarpusavyje susietų technologinių sprendimų, organizacinių procesų, duomenų mainų ir valdymo mechanizmų visuma, sudaranti sąlygas teikti, koordinuoti ir administruoti sveikatos priežiūros paslaugas skaitmeninėje aplinkoje (Adler-Milstein ir kt., 2015). Ji apima elektroninių sveikatos įrašų tvarkymą, klinikinių duomenų registravimą ir naudojimą, e. receptų ir siuntimų valdymą, laboratorinių tyrimų duomenų mainus, pacientų įtraukimą per portalus ir nuotolines paslaugas, taip pat tarpinstitucinę sąveiką per sveikatos informacijos mainų infrastruktūrą (*angl. Health Information Exchange, HIE*) (Vest ir Gamm, 2010; Reisman, 2017).

Kibernetinio saugumo valdymo požiūriu e. sveikatos sistema turi būti analizuojama kaip kompleksinė socio-techninė ekosistema, kurioje technologiniai komponentai, klinikiniai procesai, sveikatos priežiūros specialistų elgsena, pacientų prieigos kanalai, duomenų mainai, reguliacinė aplinka ir organizacinės atsakomybės yra glaudžiai tarpusavyje susiję. Socio-techninis požiūris leidžia e. sveikatą vertinti ne tik kaip techninę infrastruktūrą, bet ir kaip valdymo sistemą, kurioje informacinės technologijos palaiko paslaugų teikimą, sprendimų priėmimą, duomenų valdymą ir pacientų dalyvavimą sveikatos priežiūros procese (Sittig ir Singh, 2010; Cresswell ir Sheikh, 2013).

Tokia perspektyva ypač svarbi kuriant kibernetinio saugumo valdymo modelį, nes sveikatos priežiūros sistemų pažeidžiamumą lemia ne tik techninės spragos, bet ir pasenusi infrastruktūra, nepakankamos investicijos, žmogiškosios klaidos, darbuotojų pasirengimo trūkumas, fragmentuotos atsakomybės ir silpna saugumo kultūra (Ewoh ir Vartiainen, 2024; Hasegawa ir kt., 2024; O'Brien ir kt., 2024). Todėl e. sveikatos sistemos struktūra nagrinėjama kaip organizacinė valdymo sistema, kurioje kibernetinio saugumo veiksmingumas priklauso nuo technologijų, procesų, žmonių ir atsakomybių suderinamumo.

E. sveikatos sistemos struktūrą kibernetinio saugumo valdymo požiūriu tikslinga analizuoti pagal kelis tarpusavyje susijusius sluoksnius. Pirmasis – infrastruktūrinis sluoksnis, kurį sudaro nacionalinės ir institucinės informacinės sistemos, duomenų centrai, debesijos paslaugos, tinklo infrastruktūra, autentifikavimo sprendimai, integracinės platformos, darbo vietos ir medicininiai įrenginiai. Šis sluoksnis užtikrina techninį sistemos veikimą, tačiau kartu sukuria kritinius prieinamumo, konfigūracijų valdymo, tiekimo grandinės, atsarginių kopijų ir veiklos tęstinumo rizikos taškus (Casanova ir kt., 2025).

Antrasis – duomenų sluoksnis, apimantis elektroninius sveikatos įrašus, laboratorinių tyrimų rezultatus, diagnostinius vaizdus, e. receptus, siuntimus, registracijos duomenis, pacientų tapatybės ir prieigos informaciją. Šiame sluoksnyje svarbiausios kibernetinio saugumo dimensijos yra duomenų konfidencialumas, vientisumas, autentiškumas, atsekamumas ir teisėtas naudojimas. Duomenų sluoksnio pažeidimai sveikatos sektoriuje turi ne tik informacinį ar reputacinį, bet ir klinikinį poveikį, nes neteisingi, neprieinami ar pakeisti duomenys gali paveikti diagnostikos, gydymo ir sprendimų priėmimo procesus (Ewoh ir Vartiainen, 2024).

Trečiasis – taikomųjų paslaugų sluoksnis, kurį sudaro e. recepto, pacientų portalo, elektroninės registracijos, telemedicinos, laboratorijų, medicininių vaizdų archyvavimo, klinikinių sprendimų palaikymo ir administracinės posistemės. Šio sluoksnio saugumas priklauso nuo programinės įrangos patikimumo, sąsajų saugumo, naudotojų teisių valdymo, audito žurnalų, incidentų aptikimo ir paslaugų atkūrimo mechanizmų. Kadangi šios posistemės tiesiogiai palaiko sveikatos priežiūros paslaugų teikimą, jų sutrikimai gali lemti ne tik duomenų saugumo pažeidimus, bet ir paslaugų teikimo nutrūkimą (Pavao ir kt., 2024).

Ketvirtasis – sąveikumo sluoksnis, apimantis duomenų mainus tarp sveikatos priežiūros įstaigų, valstybės registrų, laboratorijų, vaistinių, draudimo ar administracinių sistemų, taip pat tarptautinių ar tarpvalstybinių sveikatos duomenų mainų sprendimų. Sąveikumo sluoksnis yra vienas svarbiausių kibernetinio saugumo valdymo požiūriu, nes kiekviena sąsaja tarp sistemų yra ir funkcionalumo, ir galimo pažeidžiamumo vieta. Sąveikumo trūkumai gali lemti ne tik informacijos dubliavimą ar duomenų kokybės problemas, bet ir prieigos kontrolės, atsakomybių bei incidentų valdymo neapibrėžtumą (Casanova ir kt., 2025).

Penktasis – organizacinis ir naudotojų sluoksnis, kurį sudaro sveikatos priežiūros specialistai, pacientai, administratoriai, IT specialistai, vadovybė, išoriniai tiekėjai ir reguliacinės institucijos. Šis sluoksnis parodo, kad e. sveikatos kibernetinis saugumas negali būti suprantamas vien kaip technologinių sprendimų visuma, nes jo veiksmingumą lemia ir žmogiškasis veiksnys, saugumo kultūra, atsakomybių paskirstymas, mokymai, prieigos teisių valdymas bei organizacinė disciplina. Naujausiuose tyrimuose pabrėžiama, kad sveikatos priežiūros sistemų pažeidžiamumą dažnai lemia ne viena techninė spraga, o kelių veiksnių – žmonių, procesų, technologijų ir valdymo – sąveika (Ewoh ir Vartiainen, 2025; Alharbi ir Alkhalifah, 2025, Bracciale ir kt., 2023).

E. sveikatos sistemos veikimo principų pagrindą sudaro sveikatos duomenų gyvavimo ciklas, duomenų sukūrimas, apdorojimas, perdavimas, saugojimas, naudojimas ir antrinis panaudojimas (Hayrinen ir kt., 2008; Weiskopf ir Weng, 2013). Kiekviename šiame ciklo etape atsiranda specifinių saugumo rizikų. Duomenų sukūrimo etape aktualūs tikslumo, autentiškumo ir teisingo įvedimo klausimai; duomenų perdavimo etape – ryšio kanalų saugumas, šifravimas ir sąsajų kontrolė; saugojimo etape – prieigos valdymas, atsarginių kopijų politika, konfigūracijų saugumas ir paslaugų tęstinumas; antrinio naudojimo etape – teisėtumo, anonimizavimo, pseudonimizavimo ir duomenų minimizavimo reikalavimai. Dėl to e. sveikatos sistemos saugumas turi būti siejamas ne su pavieniu informacinės sistemos elementu, bet su visu sveikatos duomenų gyvavimo ciklu.

Šiuolaikinėje e. sveikatoje reikšmingą vaidmenį atlieka standartų ekosistema. Sveikatos duomenų mainai dažnai grindžiami HL7 šeimos standartais, įskaitant HL7 FHIR, o klinikinė dokumentacija ir terminologija siejama su SNOMED CT, LOINC, ICD klasifikatoriais ir kitomis semantinio suderinamumo priemonėmis (Benson ir Grieve, 2016; Lehne ir kt., 2019). Standartizavimas svarbus ne tik techniniam suderinamumui, bet ir kibernetinio saugumo valdymui. Aiškiai apibrėžti duomenų formatai, kodavimo sistemos, sąsajų specifikacijos ir mainų protokolai leidžia mažinti klaidų

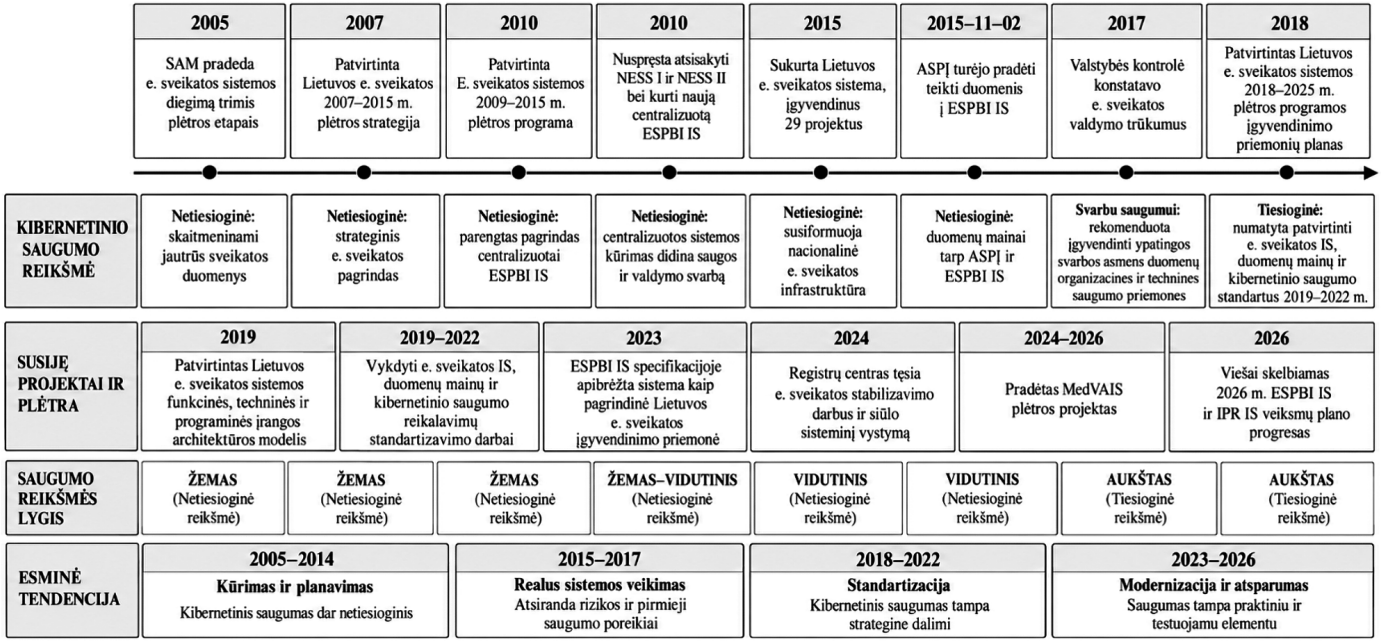
tikimybę, užtikrinti duomenų vientisumą, gerinti stebėseną ir sudaryti sąlygas nuoseklesniam prieigos bei atsakomybės valdymui.

Skirtingi e. sveikatos sistemos komponentai generuoja skirtingo pobūdžio kibernetinio saugumo rizikas. Elektroniniai sveikatos įrašai reikalauja aukšto konfidencialumo, vientisumo ir prieinamumo lygio; pacientų portalai ir mobiliosios sveikatos programėlės didina naudotojų autentifikavimo, privatumo ir duomenų naudojimo skaidrumo svarbą; sveikatos priežiūros specialistų naudojamos sistemos turi būti patikimos, prieinamos ir pritaikytos klinikinio darbo poreikiams (Al-Momani ir kt., 2024; Ikegwu ir kt., 2025). Todėl kibernetinio saugumo valdymo modelis e. sveikatos sistemoje turi apimti ne tik technines apsaugos priemones, bet ir naudotojų elgseną, organizacinį pasirengimą, rizikų vertinimą, atsakomybių paskirstymą ir veiklos tęstinumo mechanizmus.

Analizuojant e. sveikatos sistemos struktūrą, svarbu atsižvelgti ne tik į bendruosius mokslinėje literatūroje išskiriamus e. sveikatos komponentus, bet ir į konkrečios nacionalinės e. sveikatos infrastruktūros formavimosi logiką. Lietuvos atveju e. sveikatos sistema formavosi palaipsniui, pereinant nuo strateginio planavimo ir atskirų skaitmenizavimo iniciatyvų prie centralizuotos nacionalinės e. sveikatos infrastruktūros, duomenų mainų tarp asmens sveikatos priežiūros įstaigų ir nacionalinės infrastruktūros, sistemų standartizavimo, stabilizavimo ir modernizavimo. Ši raidos logika reikšminga kibernetinio saugumo požiūriu, nes saugumo svarba didėjo kartu su sistemos funkciniu, technologiniu ir instituciniu sudėtingumu.

Lietuvos e. sveikatos sistemos struktūrą tikslinga analizuoti kaip istoriškai susiformavusią nacionalinės reikšmės skaitmeninę infrastruktūrą. Iš pradžių buvo formuojami strateginiai ir programiniai e. sveikatos plėtros pagrindai, vėliau pereita prie centralizuotos ESPBI IS kūrimo ir duomenų mainų tarp sveikatos priežiūros įstaigų bei nacionalinės infrastruktūros, o pastaraisiais metais vis daugiau dėmesio skiriama standartizacijai, modernizavimui, veiklos tęstinumui ir kibernetiniam atsparumui. Tokia raida rodo, kad e. sveikatos sistema Lietuvoje palaipsniui transformavosi iš skaitmenizavimo projekto į kritinės reikšmės informacinę ekosistemą, kurios patikimumas tiesiogiai priklauso nuo kibernetinio saugumo valdymo brandos.

Toks sluoksninis ir socio-techninis e. sveikatos sistemos aiškinimas leidžia pagrįsti, kodėl kuriamas kibernetinio saugumo valdymo modelis turi būti daugiamatis. Jis turi apimti techninių kontrolės priemonių taikymą, duomenų valdymą, sąveikumo kontrolę, naudotojų prieigos valdymą, atsakomybių paskirstymą, incidentų valdymą, organizacinės brandos vertinimą ir paslaugų tęstinumo užtikrinimą. Būtent šių komponentų tarpusavio priklausomybė sudaro teorinį pagrindą toliau analizuoti Lietuvos e. sveikatos sistemos raidą, jos struktūrinius komponentus ir kibernetinio saugumo reikšmę (2 pav.).



2 pav. Lietuvos e. sveikatos sistemos raida ir kibernetinio saugumo reikšmė 2005–2026 m.

Šaltinis: sudaryta autorės, remiantis Valstybės kontrolės ataskaitomis (2008, 2011, 2017), Lietuvos Respublikos sveikatos apsaugos ministro įsakymais (2007-10-09 Nr. V-811; 2010-02-22 Nr. V-151), Lietuvos e. sveikatos sistemos 2018–2025 m. plėtros programos įgyvendinimo priemonių planu (2018)

Kaip matyti 2 paveiksle, Lietuvos e. sveikatos sistemos raida gali būti suskirstyta į kelis pagrindinius etapus. 2005 – 2014 m. laikotarpis laikytinas kūrimo ir planavimo etapu. Šiuo laikotarpiu buvo pradėta e. sveikatos sistemos diegimo plėtra, patvirtinta Lietuvos e. sveikatos 2007 – 2015 m. plėtros strategija, parengta e. sveikatos sistemos 2009 – 2015 m. plėtros programa ir priimtas sprendimas atsisakyti ankstesnių NESS I ir NESS II projektų bei kurti naują centralizuotą ESPBI IS. Šiame etape kibernetinio saugumo reikšmė dar buvo daugiausia netiesioginė, tačiau jau atsirado pagrindinės prielaidos vėlesniam saugumo poreikiui (jautrių sveikatos duomenų skaitmeninimas, centralizuotos infrastruktūros planavimas ir strateginis sveikatos informacijos valdymo pagrindas).

2015 – 2017 m. laikotarpis žymi perėjimą nuo planavimo prie realaus sistemos veikimo. Sukūrus Lietuvos e. sveikatos sistemą ir asmens sveikatos priežiūros įstaigoms pradėjus teikti duomenis į ESPBI IS, e. sveikata tapo praktikoje veikiančia nacionaline sveikatos duomenų infrastruktūra. Šiame etape išryškėjo, kad technologinės sistemos sukūrimas savaime neužtikrina efektyvaus jos valdymo. Duomenų mainai tarp įstaigų ir centrinės infrastruktūros padidino priklausomybę nuo informacinių sistemų prieinamumo, duomenų tikslumo, naudotojų prieigos valdymo ir atsakomybių tarp institucijų aiškumo. Tai dera su mokslinėje literatūroje pabrėžiama nuostata, kad e. sveikatos sistemos saugumas priklauso ne tik nuo techninių kontrolės priemonių, bet ir nuo organizacinių procesų bei naudotojų elgsenos (Cresswell ir Sheikh, 2013; Bada ir Nurse, 2020).

2018 – 2022 m. laikotarpis gali būti vertinamas kaip standartizacijos etapas, kai e. sveikatos kibernetinis saugumas tampa strategine sistemos plėtros dalimi. Šiuo laikotarpiu patvirtintas Lietuvos e. sveikatos sistemos 2018 – 2025 m. plėtros programos įgyvendinimo priemonių planas, numatyti e. sveikatos informacinių sistemų, duomenų mainų ir kibernetinio saugumo standartizavimo darbai, taip pat parengtas funkcinės, techninės ir programinės įrangos architektūros modelis. Šiame etape išryškėja perėjimas nuo fragmentiško skaitmenizavimo prie labiau standartizuotos ir architektūriškai apibrėžtos e. sveikatos sistemos. Tai svarbu kibernetinio saugumo valdymui, nes standartizavimas leidžia aiškiau apibrėžti sąsajas, duomenų formatus, naudotojų vaidmenis, prieigos teises ir saugumo kontrolės priemonių taikymo ribas.

2023 – 2026 m. laikotarpis gali būti apibūdinamas kaip modernizacijos ir atsparumo stiprinimo etapas. Šiuo laikotarpiu ESPBI IS specifikacijoje apibrėžiamas sisteminis Lietuvos e. sveikatos įgyvendinimo pagrindas, tęsiami e. sveikatos stabilizavimo darbai, pradedamas MedVAIS plėtros projektas, viešai skelbiama informacija apie ESPBI IS ir IPR IS veiksmų plano pažangą. Šiame etape kibernetinis saugumas tampa ne tik reguliaciniu ar techniniu reikalavimu, bet praktiniu e. sveikatos sistemos veikimo ir atsparumo elementu. Tai ypač svarbu atsižvelgiant į tai, kad šiuolaikinė e. sveikatos infrastruktūra apima ne tik elektroninius sveikatos įrašus, bet ir pacientų portalus, nuotolines paslaugas, mobiliąsias programėles, duomenų mainų sąsajas, klinikines technologijas ir medicininius įrenginius, kurie išplečia galimą atakos paviršių (Sood ir Enbody, 2014; Sametinger ir kt., 2015; Haleem ir kt., 2021).

Lietuvos e. sveikatos sistemos raidos analizė leidžia teigti, kad jos struktūra susiformavo kaip kelių tarpusavyje susijusių elementų visuma: centralizuotos nacionalinės infrastruktūros, asmens sveikatos priežiūros įstaigų informacinių sistemų, duomenų mainų mechanizmų, e. recepto, išankstinės pacientų registracijos, pacientų prieigos kanalų, standartizavimo dokumentų, techninės architektūros ir valdymo procesų. Todėl e. sveikatos sistemos kibernetinis saugumas negali būti analizuojamas tik kaip techninių apsaugos priemonių rinkinys. Jis turi būti vertinamas kaip sistemos valdymo gebėjimas užtikrinti duomenų konfidencialumą, vientisumą, prieinamumą, paslaugų tęstinumą, institucijų sąveiką ir atsakomybės paskirstymą visoje e. sveikatos ekosistemoje.

Atsižvelgiant į šią raidą, galima išskirti esminę teorinę prielaidą, kuo labiau e. sveikatos sistema centralizuojama, integruojama ir naudojama kasdieniuose sveikatos priežiūros procesuose, tuo didesnę reikšmę įgyja sisteminis kibernetinio saugumo valdymas. Ankstyvuosiuose e. sveikatos kūrimo etapuose saugumas daugiausia buvo susijęs su skaitmeninamų duomenų apsauga, tačiau modernizacijos etape jis tampa būtina visos sistemos patikimumo, veiklos tęstinumo ir atsparumo sąlyga. Būtent ši raidos logika pagrindžia poreikį kurti ne bendro pobūdžio, o e. sveikatos sistemos struktūrai, jos duomenų srautams, naudotojų vaidmenims, institucinei sąveikai ir veiklos tęstinumo poreikiams pritaikytą kibernetinio saugumo valdymo modelį.

Svarbus e. sveikatos veikimo principas yra identiteto, autentifikavimo ir prieigos valdymo mechanizmai, leidžiantys suderinti du iš pirmo žvilgsnio prieštaringus reikalavimus, didelį paslaugų prieinamumą sveikatos priežiūros specialistams ir griežtą jautrių asmens sveikatos duomenų apsaugą (De Hert ir kt., 2021). Sveikatos priežiūros specialistams, pacientams, vaistininkams, laboratorijų darbuotojams, administratoriams ir techniniams naudotojams reikalingos skirtingos prieigos teisės, todėl e. sveikatos sistemoje būtina taikyti vaidmenimis grįstą prieigos valdymą, mažiausių teisių principą, patikimą autentifikaciją, veiksmų auditą ir išimčių valdymą skubios pagalbos atvejais (Appari ir Johnson, 2010). Prieigos kontrolės nepakankamumas e. sveikatos sistemoje gali lemti ne tik konfidencialumo pažeidimus, bet ir duomenų vientisumo, paslaugų tęstinumo bei pacientų pasitikėjimo problemas.

Kitas ryškus e. sveikatos struktūros bruožas – medicininių prietaisų ir klinikinių technologijų integracija. IoMT (angl. *Internet of Medical Things*) plėtra, apimanti pacientų stebėsenos įrenginius, infuzines pompas, implantų valdiklius, nuotolinės stebėsenos priemones, diagnostikos įrangą ir kitus tinkluose veikiančius medicininius įrenginius, didina paslaugų efektyvumą, tačiau kartu išplečia kibernetinio saugumo rizikų lauką (Haleem ir kt., 2021; Camara ir kt., 2015, Kim ir kt. 2024). Tyrimai rodo, kad klinikinės technologijos atneša į e. sveikatos infrastruktūrą specifinių rizikų, neteisėtą prieigą, prietaisų konfigūracijos klaidas, programinės įrangos atnaujinimų trūkumus, tiekimo grandinės priklausomybes, o kai kuriais atvejais – tiesioginę grėsmę pacientų saugai, jei sutrinka prietaiso veikimas ar duomenų tikslumas (Sood ir Enbody, 2014; Sametinger ir kt., 2015). Dėl to e. sveikatos sistemos struktūros analizė turi apimti ne tik klasikinę informacinių technologijų infrastruktūrą, bet ir klinikinių technologijų valdymą, jų gyvavimo ciklą bei tiekimo grandinės kontrolę.

E. sveikatos sistemos taip pat pasižymi tuo, kad jos vienu metu aptarnauja kelias suinteresuotąsias grupes, sveikatos priežiūros įstaigas, specialistus, pacientus, valstybines institucijas, laboratorijas, vaistines, technologijų tiekėjus ir priežiūros institucijas. Ši daugiaveiksnė aplinka formuoja sudėtingą atsakomybių tinklą, kuriame saugumo valdymo spragos dažnai atsiranda tarp organizacijų, ten, kur pasibaigia vienos institucijos atsakomybė ir prasideda kitos (Bada ir Nurse, 2019; Reisman, 2017). Mokslinėje literatūroje pabrėžiama, kad būtent tarpinstitucinės sąsajos – registrų integracija, laboratoriniai užsakymai, e. receptų srautai, siuntimai ir konsultacijos yra kritinės tiek paslaugų tęstinumui, tiek saugumo valdymui (Vest ir Gamm, 2010; Adler-Milstein ir kt., 2015, Bromiley ir kt., 2015). Todėl e. sveikatos kibernetinis saugumas negali būti užtikrinamas tik vienos organizacijos pastangomis, jis reikalauja koordinuoto valdymo, bendrų standartų, aiškių atsakomybių ir nuoseklaus informacijos srautų valdymo.

E. sveikatos sistemos veikimo principai taip pat susiję su paslaugų tęstinumu. Skirtingai nei daugelyje kitų sektorių, sveikatos priežiūroje informacinių sistemų neprieinamumas gali tiesiogiai paveikti pacientų registraciją, receptų išrašymą, tyrimų rezultatų gavimą, konsultacijų organizavimą, diagnostikos procesus ir gydymo sprendimų priėmimą. Todėl e. sveikatos sistemos kibernetinio saugumo valdymas turi apimti ne tik prevencines apsaugos priemones, bet ir veiklos tęstinumo, atsarginių kopijų, atkūrimo po incidentų, alternatyvių darbo procedūrų ir komunikacijos su naudotojais mechanizmus. Šis aspektas ypač svarbus vertinant e. sveikatos sistemos atsparumą, nes atsparumas reiškia ne tik gebėjimą išvengti incidentų, bet ir gebėjimą išlaikyti kritines paslaugas, greitai atkurti veiklą ir mokytis iš sutrikimų.

Atskira e. sveikatos sistemos kibernetinio saugumo problema yra susijusi su medicininių įrenginių ir IoMT (angl. *Internet of Medical Things*) ekosistemos plėtra. Tinkliniai medicininiai įrenginiai, pacientų stebėsenos sistemos, diagnostikos prietaisai, mobiliosios sveikatos programėlės ir kiti IoMT komponentai išplečia e. sveikatos sistemos funkcionalumą, tačiau kartu padidina atakos paviršių ir sukuria naujus pacientų saugos bei duomenų apsaugos iššūkius (Menon, 2026; Freyer ir kt., 2024; Švandova ir Smutny, 2024, Bialas, 2016). Šių įrenginių saugumas negali būti vertinamas tik kaip techninė gamintojo atsakomybė, nes jų veikimas tiesiogiai susijęs su klinikiniais procesais, naudotojų elgsena, tinklo architektūra ir organizacijos incidentų valdymo pajėgumais.

Todėl e. sveikatos sistemos kibernetinio saugumo valdymo modelyje būtina numatyti atskirą IoMT ir medicininių įrenginių rizikos vertinimo dimensiją. Tokia dimensija turėtų apimti įrenginių identifikavimą, pažeidžiamumų stebėseną, programinės įrangos atnaujinimų valdymą, tinklo segmentavimą, prieigos kontrolę, tiekėjų atsakomybės apibrėžimą ir incidentų poveikio pacientų saugai vertinimą (Jaidi ir kt., 2025; Menon, 2026, Nifakos ir kt., 2021). Šis požiūris leidžia kibernetinį saugumą susieti ne tik su informacijos apsauga, bet ir su klinikinės rizikos valdymu.

Atsižvelgiant į e. sveikatos sistemos struktūrinį daugiasluoksniškumą, jos veikimo principus tikslinga apibendrinti išskiriant pagrindinius sistemos komponentus, jų atliekamas funkcijas ir tipinius kibernetinio saugumo valdymo taškus. 6 lentelėje pateikiama ši analitinė struktūra sudaro pagrindą tolesnei informacinių sistemų sąveikos,

duomenų apsaugos ir kibernetinio saugumo valdymo aspektų analizei 1.4.2–1.4.3 poskyriuose, taip pat pereinant prie kibernetinio saugumo valdymo modelio struktūros kūrimo 2 skyriuje.

6 lentelė. E. sveikatos sistemos struktūriniai komponentai ir jų veikimo logika kibernetinio saugumo valdymo požiūriu

Struktūrinis komponentas	**Pagrindinė funkcija e. sveikatoje**	**Tipiniai duomenų srautai**	**Kritinės valdymo vietos kibernetinio saugumo požiūriu**
Elektroniniai sveikatos įrašai (angl. EHR)	Klinikinės informacijos kaupimas ir panaudojimas	Klinikiniai įrašai, receptai, tyrimų rezultatai	Prieigos valdymas, auditas, duomenų vientisumas, veiklos tęstinumas (Hayrinen ir kt., 2008; Weiskopf ir Weng, 2013)
Sveikatos informacijos mainai (angl. HIE)	Tarpinstituciniai duomenų mainai	Siuntimai, epikrizės, laboratoriniai duomenys	Sąsajų valdymas, grandininė rizika, trečiųjų šalių priklausomybės (Vest ir Gamm, 2010; Adler-Milstein ir kt., 2015)
Terminologijos ir kodavimo sistemos	Semantinis suderinamumas	SNOMED CT/LOINC/ ICD žymos	Duomenų kokybė, klaidų prevencija, klinikinės interpretacijos rizika (Lehne ir kt., 2019; Benson ir Grieve, 2016)
Identiteto ir prieigos valdymas (angl. IAM)	Vartotojų identifikavimas ir teisių kontrolė	Prisijungimai, vaidmenys, sesijos	RBAC, „mažiausių teisių“ principas, išimtys skubos atvejais (Appari ir Johnson, 2010)
Klinikinės technologijos ir IoMT	Paciento stebėsena, diagnostika, terapija	Telemetrija, prietaisų parametrai	Atnaujinimų valdymas, segmentavimas, tiekėjo rizika, pacientų sauga (Haleem ir kt., 2021; Camara ir kt., 2015)
Pacientų portalai ir nuotolinės paslaugos	Paciento įtraukimas, savitarnos paslaugos	Registracijos, konsultacijos, pranešimai	Tapatybės apsauga, privatumas, saugus ryšys, socialinė inžinerija (Greenhalgh ir kt., 2017; Sheikh ir kt., 2021)
Duomenų platformos (debesija / duomenų centrai)	Duomenų saugojimas	Atsarginės kopijos, archyvai, analitika	Paslaugų tęstinumas, konfigūracijų kontrolė, tiekėjų atsakomybė (Radanliev ir kt., 2019; Gordon ir kt., 2021)

Šaltinis: sudaryta autorės, remiantis nurodytais moksliniais šaltiniais lentelėje

Apibendrinant 1.4.1 poskyrį, galima teigti, kad Lietuvos e. sveikatos sistemos struktūra atskleidžia esminę kibernetinio saugumo valdymo dilemą. Centralizuota infrastruktūra sudaro prielaidas vienodesniems duomenų mainams, bendrų standartų taikymui ir nacionalinio lygmens koordinavimui, tačiau kartu didina priklausomybę nuo centrinės sistemos prieinamumo, tinkamo prieigos valdymo ir tarpinstitucinio incidentų koordinavimo. Kibernetinio saugumo požiūriu centralizacija nėra savaime nei privalumas, nei trūkumas, jos veiksmingumas priklauso nuo to, ar kartu sukuriami aiškūs atsakomybių paskirstymo, stebėsenos, atsarginių procedūrų ir veiklos tęstinumo mechanizmai. Todėl kuriamas kibernetinio saugumo valdymo modelis turi būti orientuotas ne tik į atskirų organizacijų saugumo brandos vertinimą, bet ir į visos e. sveikatos ekosistemos tarpusavio priklausomybių, rizikos taškų ir koordinavimo mechanizmų analizę.

1.4.2. Informacinių sistemų integracija ir sąveika

Informacinių sistemų integracija ir jų tarpusavio sąveika sudaro vieną esminių e. sveikatos infrastruktūros veikimo prielaidų. Skaitmenizuotoje sveikatos priežiūros aplinkoje atskiros informacinės sistemos neveikia izoliuotai, klinikiniai sprendimai, administraciniai procesai, duomenų analizė ir paslaugų koordinavimas grindžiami nuolatiniu informacijos judėjimu tarp skirtingų technologinių komponentų, organizacijų ir naudotojų grupių. Todėl e. sveikatos sistemų sąveika turi būti vertinama ne tik kaip techninis duomenų perdavimo mechanizmas, bet ir kaip kompleksinis organizacinis bei saugumo valdymo procesas.

Sąveikumas paprastai apibrėžiamas trimis tarpusavyje susijusiais lygmenimis, techniniu, semantiniu ir organizaciniu. Techninis sąveikumas apima sistemų gebėjimą keistis duomenimis naudojant standartizuotus protokolus, sąsajas ir duomenų mainų sprendimus. Semantinis sąveikumas reiškia perduodamos informacijos reikšmės išsaugojimą ir vienodą interpretavimą skirtingose sistemose. Organizacinis sąveikumas siejamas su procesų, atsakomybių, taisyklių ir sprendimų priėmimo mechanizmų suderinimu tarp dalyvaujančių institucijų. E. sveikatos sistemose šie lygmenys persidengia, todėl bet kurios grandies trūkumas gali tapti ne tik techninio neveikimo, bet ir kibernetinio pažeidžiamumo šaltiniu.

Kibernetinio saugumo valdymo požiūriu sąveikumas e. sveikatos sistemoje turi dvigubą reikšmę. Viena vertus, jis yra būtina integruotų, tęstinių ir pacientui orientuotų sveikatos priežiūros paslaugų sąlyga. Kita vertus, kiekviena sąsaja tarp informacinių sistemų didina atakos paviršių, apsunkina atsakomybių ribų nustatymą ir kelia papildomus duomenų vientisumo, prieigos kontrolės, stebėsenos bei incidentų atsekamumo reikalavimus. Dėl šios priežasties e. sveikatos sąveikumas turi būti vertinamas ne tik funkciniu, bet ir rizikų valdymo požiūriu (Casanova ir kt., 2025; Ewoh ir Vartiainen, 2024).

Fragmentuotos sveikatos informacinės sistemos dažnai sukuria situaciją, kai duomenys juda tarp skirtingų platformų, tačiau nėra pakankamai aišku, kas atsakingas už sąsajos saugumą, audito duomenų analizę, incidento eskalavimą ar prieigos teisių

peržiūrą. Tokia fragmentacija didina riziką, kad kibernetinis saugumas bus valdomas atskirų organizacijų ar posistemių lygmeniu, bet ne visos e. sveikatos ekosistemos mastu. Todėl kuriamas kibernetinio saugumo valdymo modelis turi apimti ne tik organizacijos vidaus saugumo kontrolę, bet ir tarpinstitucinių duomenų mainų, sistemų integracijos, tiekėjų valdymo ir incidentų koordinavimo mechanizmus (van der Lei, 1991, Pavao ir kt., 2024; Garcia-Perez ir kt., 2023).

Kritiniu požiūriu sąveikumo problema parodo, kad e. sveikatos sistemos saugumas negali būti užtikrinamas vien lokaliomis techninėmis priemonėmis. Net jeigu atskira sveikatos priežiūros įstaiga turi brandžią informacijos saugumo valdymo sistemą, jos saugumas priklauso ir nuo kitų ekosistemos dalyvių, nacionalinės infrastruktūros, integracinių sąsajų, išorinių tiekėjų, vaistinių, laboratorijų, valstybės registrų ir pacientų prieigos kanalų. Todėl e. sveikatos kibernetinio saugumo valdymui būtinas ekosisteminis požiūris, apimantis bendras taisykles, koordinuotą incidentų valdymą, suderintus brandos vertinimo kriterijus ir aiškiai apibrėžtas atsakomybės ribas.

Integracijos sudėtingumas e. sveikatos srityje tiesiogiai susijęs su didesniu pažeidžiamumu. Kuo daugiau sistemų, sąsajų ir organizacijų dalyvauja duomenų mainuose, tuo sudėtingesnis tampa prieigos valdymas, atsekamumas, pokyčių kontrolė ir incidentų lokalizavimas. Skirtingais laikotarpiais sukurti sprendimai dažnai pasižymi nevienodu saugumo brandos lygiu, o jų integravimas be vieningos architektūrinio valdymo logikos gali suformuoti sunkiai kontroliuojamą priklausomybių tinklą. Tokiose aplinkose net nedidelė konfigūracijos klaida ar trečiosios šalies saugumo spraga gali turėti neproporcingai didelį poveikį visai e. sveikatos ekosistemai.

Svarbiu sąveikos aspektu tampa duomenų srautų stebėsena ir atsekamumas. Disertacijos kontekste stebėsena suprantama ne tik kaip techninis duomenų srautų stebėjimas realiuoju laiku, bet ir kaip sistemingas įvykių registravimas, analizė ir galimybė atkurti veiksmų seką po incidento. Atsekamumas reiškia gebėjimą nustatyti, kas, kada, kokiu pagrindu ir kokius sveikatos duomenis pasiekė, pakeitė ar perdavė. Skirtingai nuo atskaitomybės, kuri siejama su atsakomybės priskyrimu organizaciniu lygmeniu, atsekamumas e. sveikatos sistemose yra techninis ir procesinis reikalavimas, būtinas saugumo incidentų tyrimui, duomenų apsaugos kontrolei ir pasitikėjimui skaitmeninėmis sveikatos paslaugomis palaikyti.

Sąveikos architektūriniai sprendimai lemia ir tai, kaip veiksmingai gali būti taikomos kibernetinio saugumo kontrolės priemonės. Centralizuoti sprendimai sudaro prielaidas vieningesnei stebėsenai, standartų taikymui ir koordinavimui, tačiau kartu padidina kritinių komponentų reikšmę. Paskirstyti sprendimai gali didinti lankstumą ir mažinti priklausomybę nuo vieno centrinio komponento, tačiau jie apsunkina matomumą, kontrolę ir bendrą incidentų koordinavimą. Todėl e. sveikatos sistemų integracija turi būti vertinama kartu su kibernetinio saugumo brandos, rizikų valdymo ir veiklos tęstinumo reikalavimais.

Siekiant struktūruotai apibendrinti informacinių sistemų sąveikos tipus, jiems būdingas rizikas ir valdymo aspektus, 7 lentelėje pateikiama analitinė sąveikos tipų, rizikų ir brandos indikatorių schema.

7 lentelė. Informacinių sistemų sąveikos tipai e. sveikatos sistemose, rizikos ir brandos indikatoriai

Sąveikos tipas	**Sąveikos apibūdinimas**	**Pagrindinės kibernetinės rizikos**	**Valdymo ir kontrolės priemonės**	**Brandos indikatoriai empiriniam vertinimui**
Taškas – taškas sąveika	Tiesioginės sąsajos tarp dviejų sistemų	Ribotas stebimumas, sudėtingas pakeitimų valdymas, didėjantis atakos paviršius	Sąsajų inventorizavimas, prieigos kontrolė, audito žurnalai	Dokumentuotos sąsajos, centralizuotas pakeitimų registras, audito įrašų analizė
Integracinė platforma	Centralizuotas duomenų srautų maršrutizavimas ir transformavimas	Kritinio komponento sutrikimo rizika, konfigūracijų klaidų poveikio mastas	Konfigūracijų valdymas, stebėsena, segmentavimas	Centralizuota stebėsena, testavimo procedūros, atsarginių kopijų politika
API sąveika	Standartizuotos sąsajos paslaugoms ir programėlėms	Netinkama autentifikacija, perteklinės prieigos teisės	API sauga, autentifikavimas, greičio ribojimas	API naudojimo stebėsena, prieigos peržiūrų reguliarumas
Tarpinstitucinė sąveika	Duomenų mainai tarp skirtingų organizacijų	Atsakomybės ribų neapibrėžtumas, grandininio poveikio rizika	Sutartiniai saugumo reikalavimai, bendros procedūros	Incidentų eskalavimo aiškumas, bendrų pratybų vykdymas
Hibridinė sąveika	Kelių architektūrų derinys	Valdymo sudėtingumas, priklausomybių gausa	Architektūrinis valdymas, rizikų prioritetizavimas	Integracijų kritiškumo klasifikavimas, brandos vertinimai

Šaltinis: sudaryta autorės, remiantis Walker ir kt. (2005), Khoumbati ir kt. (2006), Vest ir Gamm (2010), Mandel ir kt. (2016), Lehne ir kt. (2019), Jalali ir Kaiser (2018), Radanliev ir kt. (2019), Gordon ir kt. (2011)

Apibendrinant galima teigti, kad informacinių sistemų integracija ir sąveika e. sveikatos sistemose yra ne tik technologinis, bet ir kibernetinio saugumo valdymo klausimas. Sąveikos architektūra lemia stebėsenos galimybes, atsekamumą, atsakomybių paskirstymą, incidentų koordinavimą ir veiklos tęstinumo užtikrinimą. Todėl kibernetinio saugumo valdymo modelis e. sveikatos kontekste turi apimti ne pavienes sistemas, o visą tarpusavyje susietų komponentų ekosistemą. Šis aspektas ypač svarbus

nagrinėjant duomenų apsaugos ir konfidencialumo užtikrinimą, kuris detaliau analizuojamas kitame poskyryje.

1.4.3. Duomenų apsauga ir konfidencialumas sveikatos sektoriuje

E. sveikatos sistemose tvarkomi duomenys apima itin platų asmens informacijos spektrą – nuo identifikacinių duomenų iki klinikinių įrašų, diagnostinių rezultatų, genetinės informacijos ir gydymo istorijų. Šie duomenys pagal Europos Sąjungos Bendrąjį duomenų apsaugos reglamentą (BDAR) priskiriami specialių kategorijų asmens duomenims, kuriems taikomi sustiprinti apsaugos reikalavimai (Europos Parlamentas ir Taryba, 2016). Mokslinėje literatūroje pabrėžiama, kad būtent sveikatos duomenų jautrumas lemia išskirtinį jų apsaugos vaidmenį kibernetinio saugumo valdymo kontekste (Rumbold ir Pierscionek, 2017).

BDAR nustato pagrindinius asmens duomenų tvarkymo principus – teisėtumą, sąžiningumą, skaidrumą, duomenų kiekio mažinimą, tikslų apibrėžtumą ir saugojimo trukmės ribojimą (Europos Parlamentas ir Taryba, 2016). Šių principų taikymas e. sveikatos sistemose reikalauja ne tik formalaus teisinio atitikimo, bet ir integravimo į informacinių sistemų architektūrą bei organizacinius procesus. Tyrimai rodo, kad organizacijos, kurios duomenų apsaugą traktuoja kaip techninį ar administracinį reikalavimą, dažniau susiduria su sisteminiais pažeidimais ir pasitikėjimo praradimu (Tikkinen-Piri ir kt., 2018).

Asmens duomenų apsaugos ir konfidencialumo užtikrinimas e. sveikatos srityje glaudžiai susijęs su apsaugos pagal projektavimą ir apsaugos pagal numatytuosius nustatymus principais (angl. *privacy by design ir privacy by default*). Moksliniai tyrimai pabrėžia, kad šie principai reikalauja saugumo ir privatumo sprendimus integruoti jau ankstyvuosiuose sistemų kūrimo etapuose, o ne taikyti juos kaip papildomas korekcijas po įgyvendinimo (Cavoukian, 2011; Voigt ir Von dem Bussche, 2017). Sveikatos informacinėse sistemose tai ypač aktualu dėl sudėtingų duomenų srautų ir daugybės suinteresuotųjų šalių.

Literatūroje taip pat akcentuojama, kad duomenų konfidencialumo pažeidimai sveikatos sektoriuje turi platesnes pasekmes nei kituose sektoriuose. Be tiesioginių teisinių ar finansinių nuostolių, tokie pažeidimai gali mažinti pasitikėjimą e. sveikatos paslaugomis ir neigiamai paveikti gydymo kokybę (McLeod ir Dolezel, 2018). Dėl šios priežasties duomenų apsauga tampa ne tik saugumo, bet ir klinikinės kokybės bei etikos klausimu (Mittelstadt, 2019).

Empiriniai tyrimai rodo, kad e. sveikatos įstaigos dažnai susiduria su iššūkiais įgyvendindamos BDAR reikalavimus praktikoje. Ypač sudėtinga užtikrinti nuoseklų prieigos teisių valdymą, veiksmingą incidentų registravimą ir savalaikį pranešimą apie asmens duomenų saugumo pažeidimus. Be to, telemedicinos ir nuotolinių sveikatos paslaugų plėtra išryškino papildomas rizikas, susijusias su naudotojų autentifikavimu, duomenų perdavimo saugumu ir atsakomybės pasiskirstymu tarp skirtingų paslaugų teikėjų (Iyengar ir kt., 2020).

Duomenų apsaugos poveikio vertinimas (angl. *Data Protection Impact Assessment, DPIA*) literatūroje vertinamas kaip vienas svarbiausių instrumentų, leidžiančių sistemingai identifikuoti ir valdyti su asmens duomenų tvarkymu susijusias rizikas (Wachter ir Mittelstadt, 2019). Sveikatos sektoriuje DPIA tampa neatsiejama kibernetinio saugumo valdymo dalimi, ypač diegiant naujas technologijas ar plečiant duomenų mainų apimtis (Radanliev ir kt., 2019).

Pastaraisiais metais moksliniuose tyrimuose vis daugiau dėmesio skiriama asmens duomenų apsaugos ir kibernetinio saugumo sąveikai. Pabrėžiama, kad BDAR atitiktis negali būti užtikrinama izoliuotai nuo bendros informacijos saugumo valdymo sistemos, o veiksmingiausi sprendimai pasiekiami integruojant teisinius, organizacinius ir techninius aspektus į vieningą valdymo modelį (Gurses ir kt., 2021; Shojaei ir kt., 2024). Tokia integracija ypač svarbi e. sveikatos sistemoms, kuriose duomenų apsauga tiesiogiai susijusi su pacientų sauga ir paslaugų patikimumu.

Apibendrinant galima teigti, kad asmens duomenų apsauga ir konfidencialumas e. sveikatos sektoriuje yra esminė kibernetinio saugumo valdymo sudedamoji dalis. BDAR nustatyti principai ir reikalavimai sudaro normatyvinį pagrindą, tačiau jų praktinis įgyvendinimas priklauso nuo organizacijų gebėjimo integruoti duomenų apsaugą į strateginius, technologinius ir operacinius sprendimus. Šiame kontekste duomenų apsauga tampa ne tik teisinės atitikties, bet ir organizacinės brandos bei visuomenės pasitikėjimo skaitmeninėmis sveikatos paslaugomis indikatoriumi.

Apibendrinant 1.4 skyriuje nagrinėtus kibernetinio saugumo valdymo sveikatos sektoriuje aspektus, galima teigti, kad e. sveikatos sistemos pasižymi išskirtiniu kompleksiškumu, kurį lemia ne tik technologinė infrastruktūra, bet ir glaudi klinikinių, organizacinių, teisinių bei tarpinstitucinių procesų sąveika. E. sveikatos sistemų struktūra, informacinių sistemų integracija ir sąveika, taip pat asmens duomenų apsaugos ir konfidencialumo reikalavimai formuoja daugiasluoksnę aplinką, kurioje kibernetinis saugumas tampa ne pavieniu techniniu uždaviniu, o nuolatiniu valdymo procesu.

Analizuoti poskyriai parodė, kad efektyvus kibernetinio saugumo užtikrinimas sveikatos sektoriuje neįmanomas be sisteminio požiūrio, apimančio aiškiai apibrėžtas atsakomybes, koordinuotus informacijos srautus, suderintas technologines ir organizacines priemones bei nuoseklų atitikties teisės aktams užtikrinimą. Ypač svarbus vaidmuo tenka asmens duomenų apsaugai, kuri e. sveikatos kontekste tiesiogiai siejasi su pacientų sauga, paslaugų patikimumu ir visuomenės pasitikėjimu skaitmeninėmis sveikatos priežiūros paslaugomis.

1.4.4. E. sveikatos sistemos kibernetinis atsparumas ir jo operaciniai rodikliai

Sveikatos sektoriuje kibernetinis incidentas gali tiesiogiai paveikti paslaugų teikimą ir tarpinstitucinius sveikatos duomenų mainus (Pavao ir kt., 2024; Ewoh ir Vartiainen, 2024; Coventry ir Branley, 2018; Jalali ir Kaiser, 2018; Garcia-Perez ir kt., 2023, Ratwani ir kt., 2018, Saldana, 2021). Kibernetinis atsparumas šiame darbe suprantamas kaip

e. sveikatos sistemos gebėjimas numatyti kibernetines grėsmes, pasirengti galimiems sutrikimams, atlaikyti incidentų poveikį, išlaikyti kritinių paslaugų teikimą, atkurti sutrikusias funkcijas ir prisitaikyti prie pasikeitusios rizikos aplinkos. Tokia samprata remiasi kibernetinio atsparumo tyrimuose akcentuojama logika, kad atspari sistema turi ne tik apsisaugoti nuo grėsmių, bet ir išlaikyti veikimą nepalankiomis sąlygomis, atkurti funkcionalumą bei mokytis iš sutrikimų (Linkov ir kt., 2013; Francis ir Bekera, 2014; Dupont ir kt., 2023).

E. sveikatos kontekste ši samprata yra ypač svarbi, nes kibernetinių incidentų poveikis neapsiriboja duomenų konfidencialumo ar informacinių sistemų prieinamumo pažeidimu. Sveikatos sektoriaus kibernetinio saugumo tyrimuose vis dažniau pabrėžiama, kad incidentų poveikis turi būti vertinamas pacientų saugos, klinikinių procesų ir organizacinio pasirengimo požiūriu. COVID-19 pandemijos laikotarpiu išryškėję kibernetinio saugumo iššūkiai parodė, kad kritinių sveikatos paslaugų skaitmenizacija didina paslaugų prieinamumą, tačiau kartu sustiprina organizacijų priklausomybę nuo saugios ir atsparios skaitmeninės infrastruktūros (Lieneck ir kt., 2023). Kritinių sistemų apsaugos kontekste vis svarbesnis tampa ne tik reagavimas į jau įvykusius incidentus, bet ir gebėjimas strategiškai planuoti apsaugos priemones, atsižvelgiant į galimas būsimas kibernetines atakas ir infrastruktūros pažeidžiamumą (Katina ir kt., 2023).

Sveikatos priežiūros organizacijos yra patrauklus kibernetinių atakų taikinys dėl kelių priežasčių, pirmiausia jos tvarko itin jautrius ir didelės vertės sveikatos duomenis, naudoja daug tarpusavyje susietų informacinių sistemų, yra priklausomos nuo paslaugų nepertraukiamumo ir dažnai veikia ribotų finansinių bei žmogiškųjų išteklių sąlygomis (Kruse ir kt., 2017; Coventry ir Branley, 2018). Be to, sveikatos priežiūros aplinkoje informacinių technologijų saugumo reikalavimai dažnai turi būti derinami su klinikinio darbo greičio, paslaugų prieinamumo ir darbuotojų patogumo poreikiais. Tai reiškia, kad jis turi apimti gebėjimą suderinti saugumo priemones su klinikinės veiklos, pacientų saugos ir paslaugų tęstinumo reikalavimais.

Empiriniai tyrimai rodo, kad išpirkos reikalaujančios atakos (angl. *ransomware*) sveikatos sektoriuje gali sutrikdyti ne tik tiesiogiai paveiktų organizacijų veiklą, bet ir gretimų sveikatos priežiūros įstaigų darbą, nes pacientų srautai, greitosios pagalbos nukreipimai ir kritinės pagalbos procesai persiskirsto regioniniu mastu (Dameff ir kt., 2023). Tai rodo, kad e. sveikatos atsparumo vertinimas turi apimti alternatyvių darbo procedūrų veiksmingumą, incidentų aptikimo greitį, komunikaciją su pacientais ir tarpinstitucinį koordinavimą.

Kibernetinio atsparumo samprata leidžia aiškiau atskirti tradicinį kibernetinį saugumą nuo atsparumu grindžiamo saugumo valdymo. Tradicinis kibernetinio saugumo požiūris dažnai orientuojamas į prevenciją, apsaugos priemones, kontrolės mechanizmus ir atitiktį reikalavimams. Atsparumu grindžiamas požiūris pripažįsta, kad ne visų incidentų galima išvengti, todėl būtina vertinti, kaip sistema pasirengia galimiems sutrikimams, kaip greitai juos aptinka, kaip koordinuotai reaguoja, kaip atkuria veiklą ir kaip panaudoja incidentų patirtį tolesniam tobulinimui. Tokia logika atitinka Linkov (2013) siūlomą kibernetinio atsparumo metrikų sampratą, kurioje atsparumas

siejamas su gebėjimu planuoti, absorbuoti poveikį, atkurti veikimą ir prisitaikyti po sutrikimų.

Platesnis kibernetinių grėsmių tyrimų laukas taip pat rodo, kad sveikatos sektoriaus grėsmės yra dinamiškos, kintančios ir susijusios su geopolitiniais, technologiniais, organizaciniais bei socialiniais veiksniais (Piazza ir Vasudevan, 2025, Amato ir kt., 2021). Tai reiškia, kad e. sveikatos kibernetinio saugumo modelis turi būti orientuotas ne tik į žinomų rizikų kontrolę, bet ir į gebėjimą nuolat stebėti kintančią grėsmių aplinką, peržiūrėti saugumo prioritetus ir adaptuoti valdymo priemones prie naujų rizikos scenarijų.

Naujos technologijos sveikatos sektoriuje turi dvejopą reikšmę, jos gali stiprinti kibernetinio saugumo pajėgumus, tačiau kartu sukuria naujų rizikų. Dirbtinis intelektas, mašininis mokymasis, blokų grandinės technologijos ir pažangūs grėsmių aptikimo metodai gali būti taikomi anomalijų nustatymui, atakų aptikimui, rizikos prognozavimui ir saugesniems duomenų mainams, tačiau jų taikymas reikalauja skaidrumo, atsakomybės ir klinikinės rizikos valdymo principų (Patra ir Rajagopalan, 2026; Khallaf ir kt., 2025; Di Palma ir kt., 2025, Bente ir kt., 2024). Todėl technologinės inovacijos savaime nėra pakankamas kibernetinio saugumo sprendimas – jos turi būti integruojamos į platesnį organizacinį ir vadybinį saugumo modelį.

Ypač svarbu tai, kad dirbtinio intelekto ir generatyvinio dirbtinio intelekto sprendimai gali būti naudojami ne tik saugumui stiprinti, bet ir naujoms atakų formoms kurti, socialinės inžinerijos kampanijoms automatizuoti ar organizacijų duomenų spragoms išnaudoti. Naujausi tyrimai parodo, kad generatyvinis dirbtinis intelektas gali padėti spręsti sveikatos sektoriaus kibernetinio saugumo duomenų trūkumo, mokymų ir žmogiškųjų pažeidžiamumų problemas, tačiau kartu turi būti valdomas atsakingai, atsižvelgiant į privatumo, duomenų kokybės ir sprendimų paaiškinamumo reikalavimus (Jalali ir Largman, 2025). Kuriamame kibernetinio saugumo valdymo modelyje naujos technologijos traktuojamos ne kaip atskiras saugumo sluoksnis, o kaip priemonių visuma, kurios veiksmingumas priklauso nuo rizikos valdymo, organizacinės brandos ir aiškiai apibrėžtų atsakomybių.

E. sveikatos sistemos kibernetinis atsparumas šiame darbe analizuojamas per šešias tarpusavyje susijusias operacines dimensijas: pasirengimą, aptikimą, reagavimą, atkūrimą, paslaugų tęstinumą ir mokymąsi. Šios dimensijos leidžia atsparumo sąvoką perkelti iš abstraktaus teorinio lygmens į operacinį vertinimo lygmenį. Tai svarbu todėl, kad teiginys apie modelio indėlį į atsparumą turi būti pagrįstas ne vien normatyvine prielaida, bet ir aiškiais rodikliais, kurie leistų vertinti, ar organizacija tampa geriau pasirengusi kibernetinėms grėsmėms, ar greičiau aptinka incidentus, ar efektyviau reaguoja, ar greičiau atkuria paslaugas ir ar geba mokytis iš sutrikimų.

Pasirengimo dimensija apima organizacijos gebėjimą iš anksto identifikuoti rizikas, apibrėžti atsakomybes, parengti veiklos tęstinumo ir atkūrimo planus, vykdyti pratybas bei užtikrinti darbuotojų pasirengimą. E. sveikatos sistemoje pasirengimas reiškia ne tik techninių apsaugos priemonių įdiegimą, bet ir aiškų klinikinių, administracinių bei informacinių procesų koordinavimą incidentų atveju. Pasirengimo lygį gali rodyti rizikų vertinimo periodiškumas, veiklos tęstinumo plano buvimas, atkūrimo plano

testavimo dažnis, atsakingų asmenų paskyrimas ir darbuotojų mokymų aprėptis. Kibernetinio saugumo valdymo tobulinimas turi būti siejamas su organizaciniu mokymusi ir žinių valdymu, nes gebėjimas dalytis žiniomis ir idėjomis sudaro prielaidas efektyvesniems organizacijos veiklos rezultatams ir inovacijų kūrimui (Limba ir kt., 2023).

Aptikimo dimensija susijusi su gebėjimu laiku nustatyti saugumo įvykius, anomalijas, neteisėtas prieigas ar paslaugų sutrikimus. Sveikatos sektoriuje incidentų aptikimo vėlavimas gali turėti tiesioginį poveikį paslaugų tęstinumui ir sveikatos duomenų saugumui. Todėl e. sveikatos organizacijose svarbu ne tik turėti technines stebėsenos priemones, bet ir užtikrinti, kad saugumo įvykiai būtų klasifikuojami, registruojami, eskaluojami ir analizuojami. Aptikimo gebėjimą gali rodyti vidutinis incidento aptikimo laikas, registruotų saugumo įvykių skaičius, žurnalų analizės aprėptis, SIEM ar kitų stebėsenos priemonių taikymas ir incidentų registravimo pilnumas.

Reagavimo dimensija apima organizacijos gebėjimą koordinuotai valdyti incidentą nuo jo identifikavimo iki poveikio suvaldymo. Reagavimas e. sveikatos sistemoje turi būti suprantamas ne tik kaip techninis problemos šalinimas, bet ir kaip organizacinis procesas, apimantis sprendimų priėmimą, komunikaciją, atsakomybių paskirstymą ir klinikinių paslaugų tęstinumo užtikrinimą. Reagavimo gebėjimą gali rodyti vidutinis reagavimo laikas, incidentų valdymo komandos sudarymas, komunikacijos plano taikymas ir incidentų valdymo pratybų rezultatai.

Atkūrimo dimensija apima gebėjimą atkurti informacinių sistemų, duomenų, paslaugų ir klinikinių procesų veikimą po incidento. Kibernetinio atsparumo požiūriu atkūrimas yra procesas, kuriame turi būti užtikrinamas duomenų vientisumas, atsarginių kopijų patikimumas, kritinių paslaugų prioritetizavimas ir saugus grįžimas į įprastą veiklą. Atkūrimo gebėjimą gali rodyti atkūrimo laiko tikslas, atkūrimo taško tikslas, faktinis paslaugų atkūrimo laikas, atsarginių kopijų testavimo dažnis, atkūrimo testų rezultatai ir kritinių sistemų prieinamumo rodikliai.

Paslaugų tęstinumo dimensija yra ypač svarbi e. sveikatos sistemos kontekste, nes kibernetinis incidentas gali trikdyti ne tik informacinių technologijų veiklą, bet ir sveikatos priežiūros paslaugų teikimą. Paslaugų tęstinumas reiškia gebėjimą išlaikyti kritines funkcijas net tada, kai dalis informacinių sistemų ar duomenų mainų mechanizmų yra sutrikę. Ši dimensija apima alternatyvias darbo procedūras, pacientų informavimą, paslaugų atkūrimo seką ir tarpinstitucinį koordinavimą. Paslaugų tęstinumo gebėjimą gali rodyti kritinių e. sveikatos paslaugų prieinamumo procentas, neplanuotų sutrikimų trukmė, alternatyvių darbo procedūrų testavimo dažnis ir kritinių procesų priklausomybės nuo informacinių sistemų įvertinimas.

Mokymosi ir prisitaikymo dimensija apima organizacijos gebėjimą iš incidentų, pratybų, auditų ir rizikų vertinimų rezultatų formuoti korekcinius veiksmus. Atsparumas nėra statiška savybė – jis turi būti stiprinamas per nuolatinį mokymąsi, procedūrų atnaujinimą, technologinių spragų šalinimą, darbuotojų kompetencijų ugdymą ir vadovybės sprendimų koregavimą. Mokymosi gebėjimą gali rodyti atliktų analizių po incidento skaičius, įgyvendintų korekcinių veiksmų dalis, atnaujintų procedūrų skaičius, pratybų rezultatų panaudojimas ir kibernetinio saugumo brandos vertinimo pokyčiai.

Operacinis kibernetinio atsparumo vertinimas leidžia tiksliau pagrįsti, kokiu būdu kibernetinio saugumo valdymo modelis gali prisidėti prie e. sveikatos sistemos tobulinimo. Modelis neturėtų būti vertinamas kaip automatiškai didinantis atsparumą vien dėl jo sukūrimo ar teorinio pagrindimo. Jo indėlis į atsparumą pasireiškia tik tada, kai modelio elementai yra įgyvendinami praktikoje, kai rizikos yra periodiškai vertinamos, incidentai registruojami ir analizuojami, prieigos teisės reguliariai peržiūrimos, atsarginės kopijos testuojamos, veiklos tęstinumo planai tikrinami pratybose, o incidentų patirtis grąžinama į strateginį ir operacinį valdymą. Todėl šiame darbe tikslinga kalbėti ne apie automatinį atsparumo padidėjimą, bet apie modelio sudaromas prielaidas didinti e. sveikatos sistemos kibernetinį atsparumą.

Siekiant sumažinti normatyvumo riziką, kibernetinis atsparumas šiame darbe siejamas su operaciniais rodikliais, kurie gali būti naudojami modelio taikymo stebėsenai ir tolesniam empiriniam vertinimui. Šie rodikliai leidžia vertinti ne tik formalų modelio komponentų buvimą, bet ir jų veiksmingumą praktikoje. Jie taip pat sudaro pagrindą tolesniems tyrimams, kuriuose būtų galima kiekybiškai vertinti, ar modelio taikymas sumažina incidentų poveikį, sutrumpina atkūrimo laiką, padidina kritinių paslaugų prieinamumą ar pagerina organizacijos gebėjimą mokytis iš incidentų (3 pav.).



3 pav. E. sveikatos sistemos kibernetinio atsparumo operacinės dimensijos ir rodikliai

Šaltinis: sudaryta autorės, remiantis Linkov ir kt. (2013), Francis ir Bekera (2014), Jalali ir Kaiser (2018), Coventry ir Branley (2018), Garcia-Perez ir kt. (2023), Dupont ir kt. (2023)

Pateikti rodikliai (3 pav.) nėra laikomi baigtiniu ar universaliu e. sveikatos sistemos kibernetinio atsparumo matavimo rinkiniu. Jie sudaro operacinį atsparumo vertinimo pagrindą, kuris gali būti pritaikomas atsižvelgiant į konkrečios organizacijos brandą, informacinių sistemų architektūrą, teikiamų paslaugų kritiškumą ir turimus duomenis. Mažesnėms sveikatos priežiūros įstaigoms gali būti aktualu pradėti nuo bazinių rodiklių, tokių kaip atsarginių kopijų testavimas, incidentų registravimas, darbuotojų mokymai ir prieigos teisių peržiūra. Didesnėms arba nacionalinės reikšmės e. sveikatos infrastruktūros organizacijoms reikšmingesni gali būti pažangesni rodikliai, tokie kaip vidutinis incidentų aptikimo laikas, vidutinis reagavimo laikas, SIEM aprėptis, sistemų prieinamumo rodikliai ir brandos indekso pokyčiai. Tokia atsparumo samprata leidžia tiksliau pagrįsti kibernetinio saugumo valdymo modelio reikšmę e. sveikatos sistemos tobulinimui ir kartu aiškiai apibrėžti, kokiais rodikliais ateityje būtų galima empiriškai vertinti modelio poveikį.

Atlikta teorinė analizė leidžia teigti, kad e. sveikatos sistemos kibernetinio saugumo valdymas negali būti grindžiamas vien teisinių reikalavimų, standartų ar pavienių technologinių priemonių taikymu. Nors ISO/IEC standartai, TIS2 direktyva, ENISA gairės ir brandos modeliai sudaro svarbų kibernetinio saugumo valdymo pagrindą, jų praktinė vertė e. sveikatos sistemoje priklauso nuo gebėjimo susieti šiuos reikalavimus su konkrečia sistemos architektūra, duomenų srautais, naudotojų vaidmenimis, sąveikumo taškais ir paslaugų tęstinumo poreikiais (Casanova ir kt., 2025; Pavao ir kt., 2024).

Kritinė literatūros analizė rodo, kad e. sveikatos sistema suprantama kaip sociotechninė ekosistema, kurioje technologiniai komponentai, pacientų prieiga, duomenų mainai, reguliaciniai reikalavimai ir žmogiškasis veiksnys yra tarpusavyje susiję. Dėl šios sąveikos kibernetinio saugumo problemos negali būti sprendžiamos izoliuotai. Pavienės prieigos kontrolės priemonės, techninė apsauga ar atitikties procedūra nėra pakankama, jeigu nėra aiškaus duomenų valdymo, incidentų koordinavimo, atsakomybių paskirstymo ir nuolatinio brandos vertinimo mechanizmo (Ewoh ir Vartiainen, 2025; Alharbi ir Alkhalifah, 2025). Ši teorinė įžvalga yra esminė kuriamam kibernetinio saugumo valdymo modeliui. Modelis turi apimti tarpusavyje susijusias technologinės infrastruktūros, duomenų ir sąveikumo valdymo, rizikų ir incidentų valdymo, kibernetinio atsparumo bei brandos vertinimo dimensijas. Tokia struktūra leidžia pereiti nuo deklaratyvios saugumo principų analizės prie struktūruoto vadybinio instrumento, orientuoto į realias e. sveikatos sistemos veikimo sąlygas (Garcia-Perez ir kt., 2023).

Apibendrinant galima teigti, kad sveikatos sektoriaus kibernetinio saugumo problematika peržengia tradicinės informacijos apsaugos ribas. Kibernetinės grėsmės sveikatos priežiūroje yra susijusios ne tik su duomenų nutekėjimu, bet ir su pacientų sauga, klinikinių procesų tęstinumu, medicininių įrenginių patikimumu, darbuotojų elgsena, organizacine branda, tiekėjų rizika ir skaitmeninės infrastruktūros atsparumu (Piazza ir Vasudevan, 2025; Brantly, 2026; Cornejo, 2026; Lieneck ir kt., 2023). Todėl e. sveikatos kibernetinio saugumo modelis kuriamas kaip daugiadimensė valdymo sistema, o ne kaip pavienių techninių priemonių rinkinys.

Ši teorinė analizė pagrindžia disertacijoje pasirinktą modelio konstravimo logiką, kad e. sveikatos kibernetinis saugumas siejamas su infrastruktūros, duomenų, paslaugų, sąveikumo, medicininių įrenginių, naudotojų ir valdysenos lygmenimis. Tokia struktūra leidžia vertinti ne tik tai, ar organizacija formaliai atitinka saugumo reikalavimus, bet ir tai, ar ji geba numatyti, aptikti, valdyti ir sušvelninti kibernetinių incidentų poveikį sveikatos priežiūros paslaugų teikimui. Todėl šiame darbe siūlomas modelis orientuojamas į prielaidų e. sveikatos sistemos kibernetiniam atsparumui didinti, rizikoms prioritetizuoti ir saugumo brandai nuosekliai stiprinti pagrindimą.

2. KIBERNETINIO SAUGUMO VALDYMO MODELIO E. SVEIKATOS SISTEMOS TOBULINIMUI STRUKTŪROS KŪRIMAS IR TYRIMO METODOLOGIJA

2.1. Kibernetinio saugumo valdymo modelių analizė

Pirmajame disertacijos skyriuje atlikta kibernetinio saugumo sampratos, grėsmių, rizikų bei informacijos saugumo valdymo sistemų analizė atskleidė, kad šiuolaikinėse skaitmenizuotose aplinkose kibernetinis saugumas negali būti suvokiamas vien kaip techninių priemonių ar atskirų kontrolės mechanizmų visuma. Mokslinėje literatūroje vis dažniau pabrėžiama, kad būtent kibernetinio saugumo valdymo modeliai sudaro pagrindą sistemingam šių elementų integravimui. Tokie modeliai leidžia ne tik konceptualizuoti saugumo veiklas, bet ir nustatyti jų tarpusavio ryšius, prioritetus bei brandos lygius, kurie yra būtini ilgalaikiam organizacijų atsparumui didinti (Siponen ir kt., 2014; Puhakainen ir Siponen, 2010, Skjelvik ir kt., 2025). Skirtingai nei pavienės saugumo priemonės, valdymo modeliai suteikia galimybę vertinti kibernetinį saugumą kaip nuolat tobulinamą procesą, o ne kaip statinę būklę.

Kibernetinio saugumo valdymo modelių įvairovė atspindi skirtingas teorines prieigas ir praktinius taikymo kontekstus. Vieni modeliai yra orientuoti į normatyvinį reguliavimą ir atitiktį standartams, kiti – į rizikų vertinimą ir sprendimų priėmimą neapibrėžtumo sąlygomis, treti – į organizacinę brandą, procesų nuoseklumą ir nuolatinį tobulinimą (von Solms ir van Niekerk, 2013; Alshaikh, 2020). Ši įvairovė kelia esminį metodologinį klausimą: kurie modeliai ir kokiu mastu yra tinkami sudėtingoms, tarpinstitucinėms e. sveikatos sistemoms.

Sveikatos sektorius pasižymi specifinėmis savybėmis, kurios apsunkina universalių kibernetinio saugumo modelių taikymą. E. sveikatos sistemos dažnai apima didelį skaičių suinteresuotųjų šalių, sudėtingas informacinių sistemų integracijas, kritinius paslaugų tęstinumo reikalavimus ir griežtą teisinį reguliavimą. Dėl šių priežasčių literatūroje akcentuojama, kad bendro pobūdžio kibernetinio saugumo modeliai turi būti vertinami ne tik pagal jų teorinį nuoseklumą, bet ir pagal praktinį pritaikomumą konkrečiame sektoriuje (Appari ir Johnson, 2010; Kruse ir kt., 2017).

Kitas svarbus aspektas yra tai, kad dauguma plačiai taikomų kibernetinio saugumo valdymo modelių buvo sukurti orientuojantis į privačiojo sektoriaus organizacijas arba kritinę infrastruktūrą siaurąja prasme, neatsižvelgiant į sveikatos paslaugų teikimo specifiką (Sittig ir Singh, 2016; Cresswell ir Sheikh, 2013). Todėl prieš kuriant naują kibernetinio saugumo valdymo modelį e. sveikatos sistemoms, būtina kritiškai įvertinti egzistuojančius teorinius ir praktinius modelius.

Šiame disertacijos skyriuje kibernetinio saugumo valdymo modeliai analizuojami kaip konceptualios struktūros, apibrėžiančios saugumo tikslus, priemones, atsakomybes ir vertinimo kriterijus. Analizė grindžiama prielaida, kad tik sistemiškai įvertinus skirtingų modelių stipriąsias ir silpnąsias puses galima pagrįstai suformuoti modelio kūrimo principus, pritaikytus e. sveikatos sistemos tobulinimui. Todėl tolesniuose

poskyriuose bus nuosekliai nagrinėjami teoriniai kibernetinio saugumo valdymo modeliai, praktiniai modeliai, taikomi sveikatos sektoriuje, bei tarpinstituciniai sprendimai, leidžiantys vertinti saugumą platesnėje ekosistemoje.

2.1.1. Teorinių kibernetinio saugumo valdymo modelių analizė

Kibernetinio saugumo valdymo modeliai mokslinėje literatūroje formuojami kaip atsakas į augantį informacinių sistemų sudėtingumą, didėjančią kibernetinių grėsmių įvairovę ir poreikį sistemingai integruoti saugumo priemones į organizacijų valdymo struktūras. Skirtingai nei pavienės techninės saugumo kontrolės, teoriniai valdymo modeliai siekia apibrėžti nuoseklią logiką, leidžiančią planuoti, įgyvendinti, vertinti ir nuolat tobulinti kibernetinio saugumo procesus organizacijos mastu (von Solms ir van Niekerk, 2013). Moksliniai tyrimai pabrėžia, kad efektyvus kibernetinio saugumo valdymas turi apimti strateginį valdymą, organizacinius procesus, žmogiškuosius veiksnius ir rizikos vertinimą (Siponen ir kt., 2014; Alshaikh, 2020, Nguyen ir kt., 2026).

Vienas ankstyviausių teorinių požiūrių siejamas su brandos modeliais, kurių ištakos glūdi programinės įrangos inžinerijoje. Organizacijų saugumo gebėjimai vystosi palaipsniui, pereinant nuo *ad hoc* sprendimų prie formaliai apibrėžtų, valdomų ir optimizuojamų procesų (Paulk ir kt., 1993). Ši koncepcija vėliau buvo adaptuota informacijos ir kibernetinio saugumo srityje, akcentuojant procesų nuoseklumą ir valdymo brandą (Singer ir Friedman, 2014). Lygiagrečiai formavosi procesiniai modeliai, tokie kaip ISO/IEC 27001 pagrindu veikianti informacijos saugumo valdymo sistema, kuri remiasi nuolatinio gerinimo ciklu (angl. *Plan Do Check Act*). Tyrimai rodo, kad procesinis požiūris leidžia integruoti kibernetinį saugumą į kasdienę organizacijos veiklą, tačiau neretai susiduria su iššūkiais, susijusiais su praktiniu pritaikymu ir organizacine kultūra (Baskerville ir kt., 2014; Suorsa, 2024).

Vėlesniuose tyrimuose vis didesnis dėmesys skiriamas holistiniams ir tarpdisciplininiams modeliams, kurie jungia technologinius, organizacinius, teisinius ir žmogiškuosius aspektus. Tokie modeliai, kaip NIST kibernetinio saugumo pagrindų struktūra ar SABSA architektūrinė metodologija, vertinami kaip tinkami sudėtingoms, tarpinstitucinėms sistemoms, kuriose svarbus ne tik saugumo lygis, bet ir jo suderinamumas su verslo ar viešojo sektoriaus tikslais (Boyson, 2014; Aven, 2016).

Sveikatos sektoriaus kontekste mokslininkai pabrėžia, kad universalūs teoriniai modeliai turi būti vertinami kritiškai, atsižvelgiant į sektoriaus specifiką, duomenų jautrumą ir paslaugų tęstinumo reikalavimus (Sittig ir Singh, 2016; Kruse ir kt., 2017). Todėl būtina ne tik analizuoti atskirus modelius, bet ir įvertinti jų taikymo ribotumus bei galimybes integruoti skirtingus požiūrius į vieningą valdymo struktūrą.

Siekiant sistemingai palyginti pagrindinius teorinius kibernetinio saugumo valdymo modelius, toliau pateikiama analitinė 8 lentelė.

8 lentelė. Teorinių kibernetinio saugumo valdymo modelių palyginamoji analizė

Modelis	Teorinis pagrindas	Pagrindinis tikslas	Valdymo lygmuo	Stiprybės	Ribotumai	Taikymo potencialas e. sveikatoje
CMM / CMMI	Brandos teorija	Procesų brandos didinimas	Organizacinis	Aiški brandos logika, progreso matavimas	Ribotas dėmesys kontekstui	Tinkamas vertinant saugumo brandą
NIST CSF	Rizikos valdymo teorija	Rizikų identifikavimas ir valdymas	Strateginis ir operacinis	Lankstus, orientuotas į riziką	Reikalauja adaptacijos sektoriui	Aukštas, ypač kritinėms IS
ISO/IEC 27001	Procesinis valdymas	ISMS įgyvendinimas	Organizacinis	Standartizuotas, audituojamas	Formalizavimo našta	Plačiai taikomas sveikatos sektoriuje
COBIT	IT valdymo teorija	IT ir verslo tikslų derinimas	Strateginis	Aiškus valdymo struktūravimas	Kompleksiškas diegimas	Tinkamas didelėms institucijoms
SABSA	Architektūrinė teorija	Saugumo architektūros kūrimas	Strateginis–techninis	Holistinis, kontekstinis	Reikalauja aukštos kompetencijos	Perspektyvus kompleksinėms sistemoms

Šaltinis: sudaryta autorės, remiantis Paulk ir kt. (1993), von Solms ir van Niekerk (2013), Baskerville ir kt. (2014), Boyson (2014), Singer ir Friedman (2014), Kruse ir kt. (2017), Aven (2016), Suorsa (2024)

Analizuojant teorinius kibernetinio saugumo valdymo modelius matyti, kad nė vienas iš jų savaime nėra pakankamas spręsti sudėtingus e. sveikatos sistemų saugumo iššūkius. Brandos modeliai suteikia struktūrą vertinimui, procesiniai modeliai – formalų valdymo pagrindą, o holistiniai modeliai – kontekstinį lankstumą. Mokslinėje literatūroje vis dažniau pabrėžiama, kad didžiausią praktinę vertę kuria integruoti požiūriai, kurie leidžia derinti skirtingų modelių stiprybes, atsižvelgiant į sektoriaus specifiką ir organizacinę brandą (Podrecca ir kt., 2025).

2.1.2. Praktiniai kibernetinio saugumo valdymo modeliai taikomi sveikatos sektoriuje

Nors teoriniai kibernetinio saugumo valdymo modeliai suteikia struktūrinį pagrindą rizikų ir saugumo procesų analizei, jų praktinis pritaikymas sveikatos sektoriuje reikalauja papildomo kontekstinio adaptavimo (Sittig ir Singh, 2016; McLeod ir Dolezel, 2018). Praktiniai kibernetinio saugumo valdymo modeliai sveikatos sektoriuje dažniausiai formuojami ne kaip visiškai naujos koncepcijos, bet kaip teorinių

modelių, tarptautinių standartų ir reguliacinių reikalavimų kombinacijos, pritaikytos konkrečiam organizaciniam ir nacionaliniam kontekstui (Kruse ir kt., 2017). Tokie modeliai siekia suderinti formalius informacijos saugumo valdymo principus su kasdiene sveikatos priežiūros organizacijų veikla.

Empiriniai tyrimai rodo, kad viena iš dažniausiai taikomų praktikų yra ISO/IEC 27001 pagrindu veikiančių ISMS diegimas, papildant jį sektoriui būdingomis procedūromis, tokiomis kaip klinikinių sistemų prieinamumo valdymas, medicininių prietaisų saugumo kontrolė ir incidentų eskalavimo protokolai (Kellermann ir Jones, 2013). Tačiau pažymima, kad vien standartinis ISMS diegimas dažnai nepakankamai atliepia sveikatos sektoriaus dinamiką, jei nėra integruojamas su klinikiniais procesais ir organizacine kultūra (Baskerville ir kt., 2014).

Kita plačiai analizuojama praktinė kryptis – rizika grįsti valdymo modeliai, paremti NIST kibernetinio saugumo pagrindų struktūra. NIST CSF praktinis taikymas sveikatos sektoriuje leidžia lanksčiau identifikuoti prioritetines rizikas ir suderinti saugumo priemones su organizacijos strateginiais tikslais (Reeves ir kt., 2020). Ypač akcentuojamas šio modelio tinkamumas kritinių sveikatos informacinių sistemų apsaugai, kur svarbu ne tik prevencija, bet ir greitas atsistatymas po incidentų.

Pastaraisiais metais vis daugiau dėmesio skiriama organizacinio atsparumo (angl. *cyber resilience*) modeliams, kurie kibernetinį saugumą traktuoja kaip nuolatinį gebėjimą prisitaikyti prie sutrikimų, o ne kaip būseną be incidentų (Linkov ir kt., 2019). Sveikatos sektoriuje tokie modeliai ypač aktualūs dėl to, kad visiškai eliminuoti incidentų tikimybę praktiškai neįmanoma, todėl pagrindinis dėmesys skiriamas paslaugų tęstinumui ir greitam funkcionalumo atkūrimui (Radanliev ir kt., 2019). Be to, išskiriami tarpinstituciniai ir ekosisteminiai valdymo modeliai, taikomi nacionalinėse e. sveikatos sistemose. Šie modeliai orientuoti į atsakomybės pasiskirstymą tarp skirtingų subjektų, bendrų saugumo reikalavimų nustatymą ir centralizuotą incidentų koordinavimą (Bada ir Nurse, 2019). Tokie modeliai gali reikšmingai sumažinti sisteminių incidentų poveikį, tačiau jų įgyvendinimas reikalauja aukšto valdymo brandos lygio ir aiškios institucinės lyderystės (Boyson, 2014).

Svarbi praktinių modelių dalis yra žmogiškojo veiksnio integravimas. Empiriniai tyrimai patvirtina, kad sveikatos sektoriuje darbuotojų sąmoningumas, mokymai ir saugumo kultūra turi tiesioginę įtaką incidentų dažniui ir mastui (Parsons ir kt., 2017; Hadlington, 2017). Todėl praktiniai kibernetinio saugumo valdymo modeliai vis dažniau apima ne tik technines ir procesines priemones, bet ir sistemingas švietimo bei kompetencijų ugdymo programas.

Apibendrinant praktinių modelių analizę, galima teigti, kad e. sveikatos sektoriuje efektyviausi sprendimai grindžiami hibridiniais valdymo modeliais, kurie jungia standartizuotas ISMS struktūras, rizika grįstą požiūrį, brandos vertinimą ir organizacinio atsparumo principus. Siekiant struktūruotai palyginti pagrindines praktinių modelių kryptis, toliau pateikiama analitinė 9 lentelė.

9 lentelė. Praktinių kibernetinio saugumo valdymo modelių taikymas e. sveikatos sektoriuje

Modelio kryptis	Teorinis pagrindas	Pagrindiniai taikymo elementai	Stiprybės sveikatos sektoriuje	Pagrindiniai iššūkiai	Brandos vertinimas
ISMS (ISO/IEC 27001 pagrindu)	Procesinis valdymas	Politikos, rizikų vertinimas, kontrolės	Standartizacija, atitiktis	Formalizavimo našta	Aukštas
NIST CSF taikymas	Rizikos valdymas	Rizikų prioritetizavimas, reagavimas	Lankstumas, kritinių IS apsauga	Reikia adaptacijos	Aukštas
Atsparumo modeliai	Sisteminis požiūris	Tęstinumas, atkūrimas	Mažina klinikinių sutrikimų poveikį	Sudėtingas matavimas	Vidutinis–aukštas
Tarpinstituciniai modeliai	Ekosisteminis valdymas	Koordinavimas, bendri standartai	Sisteminės rizikos mažinimas	Valdymo sudėtingumas	Vidutinis
Žmogiškąjį veiksnį integruojantys modeliai	Organizacinė elgsena	Mokymai, kultūra	Incidentų prevencija	Ilgalaikis poveikis	Vidutinis

Šaltinis: sudaryta autorės, remiantis Kellermann ir Jones (2013), Baskerville ir kt. (2014), Kruse ir kt. (2017), Linkov ir kt. (2019), Radanliev ir kt. (2019), Parsons ir kt. (2017), Bada ir Nurse (2019)

Analizuojami praktiniai kibernetinio saugumo valdymo modeliai atskleidžia, kad e. sveikatos sistemų apsauga negali būti grindžiama vieno modelio taikymu. Priešingai, efektyvus saugumo valdymas reikalauja integruoti skirtingas teorines prieigas į nuoseklią, sektoriui pritaikytą valdymo struktūrą. Ši įžvalga sudaro pagrindą tolesnei tarpdisciplininių ir tarpinstitucinių kibernetinio saugumo modelių analizei, kuri plėtojama 2.1.3. poskyryje.

2.1.3. Tarpinstituciniai kibernetinio saugumo valdymo modeliai ir jų efektyvumo vertinimas

Kibernetinio saugumo valdymas skaitmenizuotose sistemose vis dažniau peržengia atskirų organizacijų ribas ir tampa tarpinstituciniu procesu, reikalaujančiu koordinuotų sprendimų, bendrų atsakomybės mechanizmų ir struktūruoto informacijos mainų užtikrinimo. Mokslinėje literatūroje pabrėžiama, kad sudėtingose socio-techninėse aplinkose, tokiose kaip e. sveikatos sistemos, izoliuotas organizacinis požiūris į kibernetinį saugumą yra nepakankamas, nes incidentų pasekmės dažnai išplinta per

institucinius, technologinius ir paslaugų teikimo tinklus (Boyson, 2014; Ransbotham ir kt., 2012). Tarpinstituciniai kibernetinio saugumo valdymo modeliai apima įvairias organizacines formas – nuo centralizuotų nacionalinių koordinavimo struktūrų iki decentralizuotų bendradarbiavimo tinklų ir hibridinių sprendimų. Šių modelių pasirinkimas ir taikymas yra glaudžiai susijęs su sektoriaus brandos lygiu, pasitikėjimo tarp institucijų laipsniu, reguliacine aplinka ir technologinės infrastruktūros sudėtingumu (Gal-Or ir Ghose, 2005; Gordon ir kt., 2016). Sveikatos sektoriuje šie veiksniai įgyja papildomą reikšmę dėl kritinių paslaugų svarbos, jautrių asmens duomenų apdorojimo ir didelio tarpusavio priklausomumo tarp skirtingų paslaugų teikėjų.

Efektyvumo vertinimas tarpinstituciniuose kibernetinio saugumo modeliuose tampa esminiu analitiniu klausimu, nes leidžia ne tik palyginti skirtingas valdymo architektūras, bet ir įvertinti jų tinkamumą konkrečiam sektoriui ar sistemai. Moksliniuose tyrimuose efektyvumas siejamas su reagavimo į incidentus greičiu, koordinavimo kokybe, informacijos dalijimosi intensyvumu, rizikų mažinimo rezultatais ir gebėjimu mokytis iš įvykusių incidentų (Kwon ir Johnson, 2014; Podrecca ir kt., 2025). Atsižvelgiant į šiuos kriterijus, toliau pateikiama analitinė 10 lentelė, leidžianti sistemingai palyginti pagrindinius tarpinstitucinių kibernetinio saugumo valdymo modelių tipus.

10 lentelė. Tarpinstitucinių kibernetinio saugumo valdymo modelių tipai ir jų efektyvumo vertinimo kriterijai

Modelio tipas	**Valdymo logika**	**Pagrindiniai privalumai**	**Esminiai ribotumai**	**Efektyvumo vertinimo kriterijai**	**Taikymo aktualumas e. sveikatos sistemose**
Centralizuotas koordinavimo modelis	Sprendimų priėmimas ir incidentų valdymas koncentruojami vienoje nacionalinėje ar sektorinėje institucijoje	Vieningos procedūros, aiškus atsakomybės paskirstymas, standartizuotas reagavimas	Ribotas lankstumas, didelė administracinė apkrova	Reagavimo laikas, procedūrų laikymosi nuoseklumas, incidentų sprendimo efektyvumas	Tinkamas nacionalinėms e. sveikatos platformoms
Decentralizuotas tinklinis modelis	Autonomiškų institucijų bendradarbiavimas per savanoriškus informacijos mainus	Didelis prisitaikymas, greitesni lokalūs sprendimai	Priklausomybė nuo pasitikėjimo, nevienodas brandos lygis	Informacijos mainų intensyvumas, pasitikėjimo lygis	Aktualus regioninėms ar specializuotoms sistemoms

Modelio tipas	Valdymo logika	Pagrindiniai privalumai	Esminiai ribotumai	Efektyvumo vertinimo kriterijai	Taikymo aktualumas e. sveikatos sistemose
Hibridinis modelis	Derinama centrinė koordinacija su instituciniu savarankiškumu	Balansas tarp kontrolės ir lankstumo	Sudėtingas valdymas, didesni koordinavimo kaštai	Koordinavimo efektyvumas, rizikų mažinimo rezultatai	Ypač tinkamas kompleksinėms e. sveikatos ekosistemoms
Informacijos dalijimosi konsorciumo modelis	Struktūruotas grėsmių ir incidentų duomenų keitimasis	Kolektyvinis mokymasis, ankstyvas grėsmių aptikimas	Teisiniai ir reputaciniai iššūkiai	Duomenų kokybė, prevencinių priemonių veiksmingumas	Naudingas tarp ligoninių ir laboratorijų
Tiekimo grandinės pagrindu veikiantis modelis	Rizikų valdymas per paslaugų ir technologijų tiekėjų ekosistemą	Geresnis trečiųjų šalių rizikų matomumas	Ribota tiesioginė kontrolė	Tiekėjų atitikties lygis, incidentų kilmės analizė	Kritiškai svarbus e. sveikatos IT platformoms

Šaltinis: sudaryta autorės, remiantis Boyson (2014), Gal-Or ir Ghose (2005), Kwon ir Johnson (2014), Gordon ir kt. (2016), Ransbotham ir kt. (2012), Podrecca ir kt. (2025), Suorsa (2024)

Lentelėje pateikta analizė atskleidžia, kad tarpinstitucinių kibernetinio saugumo valdymo modelių efektyvumas nėra universalus ir priklauso nuo kontekstinių veiksnių, tokių kaip organizacijų brandos lygis, reguliacinė aplinka ir technologinė integracija. Ypač e. sveikatos sistemose išryškėja poreikis derinti skirtingų modelių principus, nes nei griežtai centralizuotas, nei visiškai decentralizuotas požiūris negeba pilnai atliepti sektoriaus sudėtingumo ir rizikų pobūdžio.

Moksliniuose tyrimuose pažymima, kad hibridiniai valdymo sprendimai gali didinti atsparumą kibernetiniams incidentams, nes sudaro sąlygas išlaikyti strateginę kontrolę nacionaliniu ar instituciniu lygmeniu, kartu užtikrinant pakankamą operacinį lankstumą atskirose organizacijose (Gordon ir kt., 2016; Podrecca ir kt., 2025). Ši įžvalga ypač reikšminga e. sveikatos sistemoms, kuriose būtina suderinti centralizuotą koordinavimą, bendrus saugumo standartus ir lokalių sveikatos priežiūros įstaigų veiklos autonomiją.

Apibendrinant galima teigti, kad tarpinstitucinių kibernetinio saugumo valdymo modelių analizė yra svarbi tolesniam valdymo modelio kūrimui. Ji leidžia identifikuoti esmines valdymo dimensijas – koordinavimą, informacijos mainus, atsakomybės paskirstymą ir efektyvumo vertinimą – kurios vėliau bus integruojamos į kibernetinio saugumo valdymo modelio struktūrą e. sveikatos sistemos tobulinimui.

2.1 skyriuje atlikta kibernetinio saugumo valdymo modelių analizė parodė, kad šiuolaikinis požiūris į kibernetinį saugumą peržengia vien techninių priemonių taikymo ribas ir vis dažniau grindžiamas sisteminiu, organizaciniu bei tarpinstituciniu

valdymu. Teorinių modelių analizė atskleidė, kad tokie modeliai kaip NIST CSF, ISO/IEC 27001, COBIT ar SABSA suteikia struktūruotą pagrindą kibernetinio saugumo procesų planavimui, rizikų valdymui ir saugumo brandos vertinimui. Vis dėlto jų universalumas riboja tiesioginį pritaikomumą specifiniuose sektoriuose, ypač e. sveikatos sistemose, kuriose saugumo valdymas turi būti derinamas su klinikiniais procesais, duomenų jautrumu, paslaugų tęstinumu ir tarpinstitucine sąveika.

Praktinių kibernetinio saugumo valdymo modelių, taikomų sveikatos sektoriuje, analizė parodė, kad veiksmingiausi sprendimai remiasi integruotu požiūriu, apimančiu technologinius, organizacinius ir žmogiškuosius veiksnius. Šiuose modeliuose akcentuojamas paslaugų tęstinumas, duomenų apsauga, incidentų valdymas ir pacientų sauga. Tačiau dauguma praktinių modelių pirmiausia orientuoti į atskiros organizacijos lygmenį, todėl nepakankamai atspindi sudėtingą e. sveikatos ekosistemų tarpinstitucinę sąveiką, duomenų mainų priklausomybes ir bendros atsakomybės klausimus.

Tarpinstitucinių kibernetinio saugumo valdymo modelių analizė atskleidė, kad kibernetinės rizikos e. sveikatos sistemose pasižymi sisteminiu pobūdžiu ir reikalauja koordinuotų valdymo mechanizmų, grindžiamų informacijos mainais, aiškiu atsakomybių paskirstymu ir suderintais reagavimo procesais. Šių modelių veiksmingumas priklauso nuo valdymo brandos, tarpinstitucinio pasitikėjimo, aiškiai apibrėžtų vaidmenų ir bendrų vertinimo kriterijų. Vis dėlto praktikoje jų taikymą riboja metodologinio vientisumo, operacinių rodiklių ir poveikio vertinimo priemonių stoka.

Apibendrinant galima teigti, kad egzistuojantys kibernetinio saugumo valdymo modeliai sudaro svarbų teorinį ir praktinį pagrindą, tačiau nė vienas iš jų atskirai neužtikrina visapusiško e. sveikatos sistemų kibernetinio saugumo valdymo. Tai pagrindžia poreikį kurti integruotą kibernetinio saugumo valdymo modelį, kuris sujungtų teorinių modelių struktūriškumą, praktinių sprendimų pritaikomumą ir tarpinstitucinių modelių sisteminį požiūrį. Šio modelio kūrimo principai, reikalavimai ir struktūrinės prielaidos nagrinėjami 2.2. disertacijos skyriuje.

2.2. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui kūrimo principai ir reikalavimai

Kibernetinio saugumo valdymo modelio kūrimas e. sveikatos sistemų kontekste yra sudėtingas metodologinis uždavinys, reikalaujantis derinti skirtingų mokslo sričių požiūrius, tarptautinius standartus ir sveikatos sektoriaus specifiką. Veiksmingas modelis turi būti grindžiamas aiškiai apibrėžtais principais ir reikalavimais, kurie užtikrintų jo nuoseklumą, pritaikomumą ir ilgalaikį veiksmingumą (Siponen ir kt., 2009; Von Solms ir Von Solms, 2018). E. sveikatos sistemos kontekste toks modelis grindžiamas integruotu požiūriu, apimančiu strateginę valdyseną, rizikų valdymą, darbuotojų elgseną, technologinius sprendimus ir organizacinį atsparumą. Naujausi tyrimai pabrėžia, kad sveikatos sektoriui reikalingi ne universalūs, bet sektoriui pritaikyti kibernetinio saugumo vertinimo instrumentai, leidžiantys organizacijoms įsivertinti pasirengimą, identifikuoti silpnąsias vietas ir planuoti tobulinimo veiksmus (Burke ir kt., 2024; Burke, Stranieri ir Oseni, 2025). Tai ypač svarbu todėl, kad sveikatos

priežiūros organizacijos dažnai veikia ribotų finansinių, žmogiškųjų ir technologinių išteklių sąlygomis, todėl kibernetinio saugumo priemonės turi būti prioritetizuojamos atsižvelgiant į realų rizikos lygį.

Šiame kontekste kuriamas modelis neturėtų būti orientuojamas vien į atitiktį teisės aktams ar standartams. Jis turi padėti vertinti praktinį organizacijos gebėjimą valdyti kibernetines rizikas, užtikrinti paslaugų tęstinumą ir nuosekliai didinti saugumo brandą. Hibridiniai rizikų valdymo metodai leidžia derinti techninius, organizacinius ir procesinius vertinimo kriterijus, o integruotos metodikos sudaro prielaidas susieti grėsmių žvalgybą, incidentų valdymą, kritinių sistemų apsaugą ir sveikatos priežiūros paslaugų tęstinumą (Aakanksha ir Krishna, 2025; Coutinho ir kt., 2023). Todėl disertacijoje kuriamas modelis suprantamas kaip vadybinis instrumentas, skirtas ne tik rizikoms identifikuoti, bet ir sistemiškai stiprinti e. sveikatos sistemos kibernetinio saugumo valdymą.

Vienas esminių modelio kūrimo principų yra sistemiškumas. Kibernetinis saugumas turi būti traktuojamas kaip visos organizacijos valdymo sistemos dalis, susijusi su strateginiais tikslais, procesų valdymu ir organizacine kultūra (Dhillon ir Backhouse, 2001). Toks požiūris leidžia išvengti fragmentuoto saugumo priemonių diegimo, kai atskiros kontrolės priemonės taikomos izoliuotai ir nesukuria bendro organizacijos atsparumo kibernetinėms grėsmėms.

Kitas svarbus principas yra procesinis kibernetinio saugumo valdymo pobūdis. Kibernetinis saugumas turėtų būti suvokiamas kaip nuolatinis ir ciklinis procesas, apimantis saugumo veiklų planavimą, įgyvendinimą, rezultatų vertinimą ir sprendimų koregavimą atsižvelgiant į kintančią grėsmių aplinką (Aven, 2016; Singer ir Friedman, 2014). Šis principas ypač aktualus e. sveikatos sistemoms, kuriose technologiniai sprendimai, organizaciniai procesai ir reguliaciniai reikalavimai nuolat kinta.

Modelio kūrime taip pat svarbus daugiamatiškumas (Alshaikh, 2020). Daugiamatis požiūris leidžia identifikuoti ne tik technologines spragas, bet ir struktūrinius organizacijos silpnumus, kurie gali lemti kibernetinių incidentų atsiradimą arba apsunkinti jų valdymą. E. sveikatos sistemų atveju ypatingą reikšmę įgauna ir kontekstinis pritaikomumas. Universalūs kibernetinio saugumo modeliai, sukurti bendram organizacijų kontekstui, ne visada pakankamai atspindi sveikatos sektoriaus specifiką (Sittig ir Singh, 2016; Kruse ir kt., 2017). Todėl modelio kūrimo procese būtina numatyti galimybę bendruosius kibernetinio saugumo principus pritaikyti konkretiems e. sveikatos sistemos struktūriniams ir funkciniams ypatumams.

Dar vienas reikšmingas principas yra orientacija į brandą. Kibernetinio saugumo valdymo modelis turi leisti ne tik aprašyti esamą saugumo būklę, bet ir vertinti organizacijos pažangą ilgalaikėje perspektyvoje. Brandos principas leidžia diferencijuoti organizacijas pagal jų gebėjimą valdyti rizikas, reaguoti į incidentus ir mokytis iš sukauptos patirties (Kwon ir Johnson, 2014; Radanliev ir kt., 2018). Šis principas yra svarbus disertacijoje, nes sudaro metodologinį pagrindą empiriniam modelio vertinimui vėlesniuose darbo skyriuose.

Kalbant apie modelio kūrimo reikalavimus, mokslinėje literatūroje pirmiausia išskiriamas aiškumas ir struktūriškumas. Modelis turi būti suprantamas skirtingų sričių specialistams – vadovams, informacinių technologijų specialistams, kibernetinio

saugumo ekspertams ir kitiems sprendimų priėmėjams (Siponen ir Willison, 2009). Kartu jis turi būti pakankamai struktūruotas, kad leistų sistemiškai susieti strateginius tikslus, operacinius procesus, atsakomybes ir technines saugumo priemones.

Naujausi tyrimai taip pat pabrėžia vertinimo kriterijų ir rodiklių svarbą. Kibernetinio saugumo valdymo modeliai turi sudaryti prielaidas nustatyti aiškius rodiklius, kurie galėtų būti taikomi tiek organizacijos savianalizei, tiek išoriniam vertinimui (Podrecca ir kt., 2025; Suorsa, 2025). Šis reikalavimas ypač aktualus e. sveikatos sistemoms, kuriose sprendimai dėl saugumo priemonių turi būti grindžiami patikimais, palyginamais ir praktikoje pritaikomais duomenimis.

Apibendrinant galima teigti, kad kibernetinio saugumo valdymo modelio kūrimo principai ir reikalavimai sudaro pagrindą integruotam, pritaikomam ir empiriškai vertinamam modeliui formuoti. Sistemiškumas, procesinis požiūris, daugiamatiškumas ir pritaikomumas leidžia pereiti nuo abstrakčių saugumo koncepcijų prie praktinių valdymo sprendimų. Šių principų detalizavimas sudaro prielaidas kitame poskyryje nagrinėti funkcinius ir nefunkcinius reikalavimus, kurie tampa pagrindu kuriant ir vertinant kibernetinio saugumo valdymo modelį e. sveikatos sistemos tobulinimui.

2.2.1. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui funkciniai ir nefunkciniai reikalavimai

Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui funkciniai ir nefunkciniai reikalavimai sudaro metodologinį pagrindą, leidžiantį pereiti nuo teorinių koncepcijų prie praktiškai taikomo, empiriškai vertinamo modelio. Todėl, be aiškiai apibrėžtų reikalavimų bet koks valdymo modelis išlieka normatyvinis, ypač sudėtingose socio-techninėse aplinkose, tokiose kaip e. sveikatos sistemos (Hevner ir kt., 2004; Gregor ir Hevner, 2013). Funkciniai reikalavimai apibrėžia, kokias valdymo funkcijas modelis turi atlikti, o nefunkciniai reikalavimai nusako, kaip šios funkcijos turi būti įgyvendinamos, siekiant užtikrinti modelio patikimumą, pritaikomumą ir ilgalaikį tvarumą. Toks atskyrimas plačiai taikomas informacinių sistemų ir kibernetinio saugumo tyrimuose, nes leidžia struktūruotai susieti valdymo procesus su jų kokybinėmis charakteristikomis (Boehm, 1984; Thomasian ir kt., 2021).

Vienas esminių funkcinių reikalavimų, nuosekliai akcentuojamų moksliniuose tyrimuose, yra rizikų identifikavimo ir vertinimo funkcija. Kibernetinio saugumo valdymo modelis privalo sudaryti galimybes sistemingai identifikuoti grėsmes, pažeidžiamumus ir galimą poveikį organizacijos veiklai (Aven, 2016). E. sveikatos sistemų kontekste ši funkcija įgauna papildomą reikšmę, nes rizikų vertinimas turi apimti ne tik informacijos saugumo aspektus, bet ir klinikinių procesų tęstinumą bei pacientų saugą (Sittig ir Singh, 2016).

Kitas fundamentalus funkcinis reikalavimas yra incidentų valdymo funkcija, apimanti pasirengimą, aptikimą, reagavimą ir atkūrimą. Organizacijos, kurios incidentų valdymą traktuoja kaip integruotą valdymo ciklo dalį, pasižymi didesniu atsparumu ir trumpesniu paslaugų atkūrimo laiku (Tondel ir kt., 2014; Ahmad ir kt., 2015). E. sveikatos sistemose ši funkcija tiesiogiai susijusi su gebėjimu užtikrinti kritinių paslaugų

tęstinumą net ir esant kibernetiniams sutrikimams.

Ne mažiau svarbus funkcinis reikalavimas – valdymo sprendimų koordinavimo funkcija. Kibernetinis saugumas negali būti efektyviai valdomas izoliuotai informacinių technologijų padaliniuose. Būtina aiški sąveika tarp strateginio, taktinio ir operacinio lygmenų (Weill ir Ross, 2004; Von Solms ir Von Solms, 2018). Kibernetinio saugumo valdymo modelis turi užtikrinti, kad sprendimai būtų priimami remiantis bendra rizikos samprata ir organizacijos strateginiais tikslais.

Svarbi funkcinė dimensija yra atitikties ir kontrolės funkcija, leidžianti sistemingai stebėti, kaip laikomasi teisinių, reguliacinių ir vidaus politikos reikalavimų. Atitiktis pati savaime neužtikrina saugumo, tačiau jos integravimas į platesnį valdymo modelį leidžia sumažinti fragmentaciją ir padidinti procesų skaidrumą (Siponen ir Willison, 2009; Kwon ir Johnson, 2013).

Galiausiai, kibernetinio saugumo valdymo modelis turi atlikti organizacinio mokymosi funkciją. Gebėjimas analizuoti incidentus, vertinti priimtų sprendimų efektyvumą ir adaptuoti procesus yra vienas svarbiausių ilgalaikio saugumo brandos veiksnių (Ransbotham ir kt., 2012; Jarvelainen, 2013). Ši funkcija ypač aktuali e. sveikatos sektoriuje, kuriame technologiniai ir organizaciniai pokyčiai vyksta itin sparčiai.

Nefunkciniai reikalavimai apibrėžia kokybines savybes, be kurių net ir funkciškai pilnas modelis gali būti nepritaikomas praktikoje. Vienas svarbiausių nefunkcinių reikalavimų yra pritaikomumas. Kibernetinio saugumo valdymo modeliai turi būti pakankamai lankstūs, kad galėtų būti taikomi skirtingo dydžio ir brandos organizacijose (Singer ir Friedman, 2014; Radanliev ir kt., 2019). E. sveikatos sistemų atveju tai reiškia gebėjimą prisitaikyti prie skirtingų institucinių struktūrų ir technologinių sprendimų.

Kitas esminis nefunkcinis reikalavimas – skaidrumas ir aiškumas. Tyrimai rodo, kad pernelyg sudėtingi ar techniniai terminais paremti modeliai dažnai lieka neįgyvendinti praktikoje, nes nėra suprantami sprendimų priėmėjams (Dhillon ir Backhouse, 2001; Alshaikh, 2020). Todėl modelio struktūra ir terminologija turi būti aiški skirtingų kompetencijų naudotojams. Taip pat, kibernetinio saugumo valdymo modelis turi sudaryti galimybes apibrėžti rodiklius, leidžiančius empiriškai vertinti tiek esamą būklę, tiek pažangą laikui bėgant (Podrecca ir kt., 2025). Šis aspektas yra tiesiogiai susijęs su disertacijos empirine dalimi, kurioje bus vertinamas modelio taikymas praktikoje.

Literatūroje taip pat akcentuojamas integruojamumo reikalavimas. Modelis turi būti suderinamas su egzistuojančiomis informacijos saugumo valdymo sistemomis, organizaciniais procesais ir teisės aktų reikalavimais (Halamka, 2008, Von Solms ir Von Solms, 2018). Sveikatos sektoriuje tai ypač svarbu dėl daugybės tarpusavyje sąveikaujančių informacinių sistemų ir institucijų.

Galiausiai, nefunkciniai reikalavimai apima patikimumą ir tęstinumą. Tyrimai pabrėžia, kad kibernetinio saugumo valdymo modeliai turi veikti ne tik normaliomis sąlygomis, bet ir krizinėse situacijose, kai organizacijos susiduria su dideliu neapibrėžtumu ir laiko trūkumu (Bada ir Nurse, 2019; Boyson, 2014). Tai reiškia, kad modelis turi būti orientuotas į ilgalaikį atsparumą, o ne trumpalaikius sprendimus.

Apibendrinant galima teigti, kad funkciniai ir nefunkciniai reikalavimai sudaro konceptualų tiltą tarp teorinių kibernetinio saugumo valdymo modelių ir jų praktinio

taikymo e. sveikatos sistemose. Funkciniai reikalavimai apibrėžia esmines valdymo veiklas, o nefunkciniai – užtikrina, kad šios veiklos būtų įgyvendinamos nuosekliai, skaidriai ir empiriškai vertinamai. Toks reikalavimų struktūravimas sudaro metodologinį pagrindą tolesniam modelio kūrimo etapui, kuriame bus detalizuojami pritaikomumo principai, valdymo lygiai ir atsakomybių pasiskirstymas (11 lentelė).

11 lentelė. Funkcinių ir nefunkcinių kibernetinio saugumo valdymo reikalavimų sąsajos su empiriniais vertinimo indikatoriais e. sveikatos sistemos kontekste

Reikalavimų kategorija	Valdymo dimensija	Praktinė reikšmė e. sveikatos sistemoje	Empiriniai vertinimo indikatoriai	Galimas duomenų rinkimo metodas
Funkciniai reikalavimai	Rizikų identifikavimas ir vertinimas	Formalizuoti kibernetinių rizikų nustatymo ir vertinimo procesai visose e. sveikatos sistemos grandyse	Reguliariai atliekamas rizikų vertinimas (taip / ne); Rizikų vertinimo metodikos buvimas; Rizikų peržiūros periodiškumas.	Dokumentų analizė; ekspertų apklausa
	Incidentų valdymas	Nustatytos procedūros kibernetiniams incidentams aptikti, registruoti, tirti ir valdyti	Incidentų registravimo mechanizmas; Reagavimo laiko vertinimas; Incidentų analizė po įvykio (angl. *post-incident review*) praktika.	Anketinė apklausa; interviu
	Prieigos valdymas	Vartotojų prieigos teisės diferencijuojamos pagal pareigas ir funkcijas	Prieigos teisių peržiūros dažnis; Daugiafaktorės autentifikacijos taikymas; Incidentai dėl neteisėtos prieigos	Dokumentų analizė; apklausa
	Duomenų apsaugos užtikrinimas	Techninės ir organizacinės priemonės, skirtos asmens sveikatos duomenų apsaugai	Šifravimo taikymas; Duomenų atsarginių kopijų politika; Duomenų vientisumo kontrolė.	Dokumentų analizė; ekspertinis vertinimas

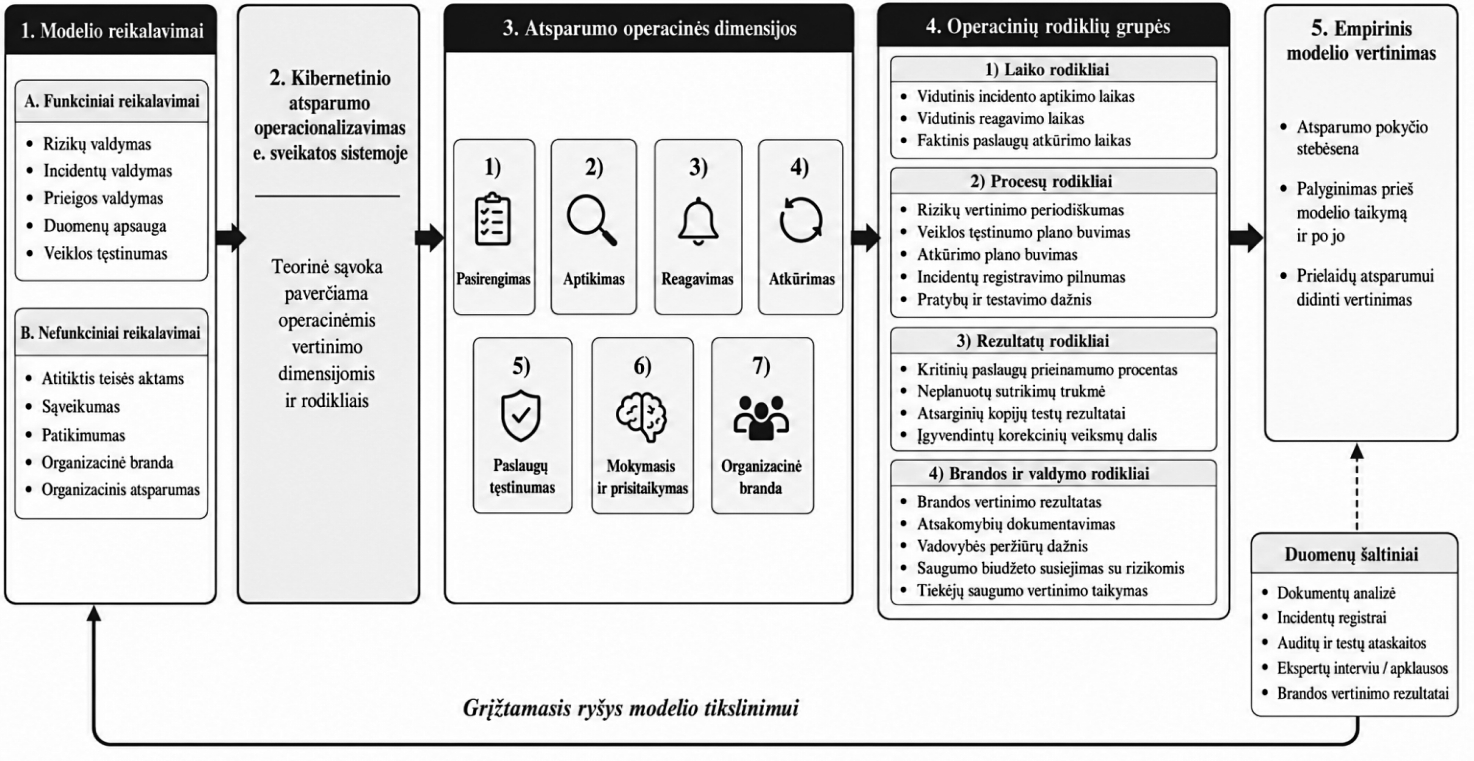
Reikalavimų kategorija	Valdymo dimensija	Praktinė reikšmė e. sveikatos sistemoje	Empiriniai vertinimo indikatoriai	Galimas duomenų rinkimo metodas
Nefunkciniai reikalavimai	Organizacinė atsakomybė	Aiškiai apibrėžti vaidmenys ir atsakomybės kibernetinio saugumo srityje	Paskirtas kibernetinio saugumo vadovas (CISO); Atsakomybių dokumentavimas; Vadovų įsitraukimas.	Interviu; dokumentų analizė
	Brandos ir nuoseklumo lygis	Kibernetinio saugumo procesų nuoseklumas ir integracija į bendrą valdymą	Procesų formalizavimo lygis; Brandos vertinimas; Integracija su IT ir klinikiniais procesais.	Apklausos; brandos vertinimo skalės
	Organizacinis atsparumas	Gebėjimas palaikyti paslaugų tęstinumą incidentų metu	Veiklos tęstinumo planai; Testavimo periodiškumas; Sistemos atkūrimo laikas.	Dokumentų analizė; ekspertų apklausa
	Žmogiškųjų išteklių kompetencijos	Darbuotojų gebėjimai atpažinti ir valdyti kibernetines grėsmes	Mokymų reguliarumas; Darbuotojų saugumo sąmoningumo vertinimas; Socialinės inžinerijos incidentų skaičius.	Apklausos; mokymų analizė
	Pritaikomumas ir lankstumas	Modelio gebėjimas prisitaikyti prie skirtingo dydžio ir brandos organizacijų	Modelio taikymo paprastumas; Reikalavimų proporcingumas; Adaptavimo galimybės.	Ekspertinis vertinimas

Šaltinis: sudaryta autorės, remiantis informacijos saugumo valdymo, kibernetinio saugumo brandos modelių ir e. sveikatos sistemų valdymo mokslinių tyrimų analize

Pateikta funkcinio ir nefunkcinio pobūdžio reikalavimų bei empirinių indikatorių sąsajų analizė leidžia sistemiškai pagrįsti kibernetinio saugumo valdymo modelio vertinimo logiką e. sveikatos sistemos kontekste. 11 lentelėje išskirti indikatoriai sudaro metodologinį pagrindą empiriniam tyrimui, nes jie leidžia vertinti ne tik techninių saugumo priemonių taikymą, bet ir organizacinių procesų brandą, valdymo nuoseklumą, atsakomybių paskirstymą, incidentų valdymą bei e. sveikatos sistemos atsparumo kibernetinėms grėsmėms prielaidas.

Kadangi kibernetinio atsparumo samprata teoriškai pagrįsta 1.4.4 poskyryje, šiame etape ji naudojama kaip vertinimo logika, leidžianti funkcinius ir nefunkcinius

modelio reikalavimus susieti su konkrečiais pasirengimo, aptikimo, reagavimo, atkūrimo, paslaugų tęstinumo ir organizacinio mokymosi rodikliais. Tokia operacionalizavimo logika leidžia susieti modelio reikalavimus su konkrečiomis atsparumo dimensijomis, rodiklių grupėmis, duomenų šaltiniais ir empirinio vertinimo galimybėmis. Tai sudaro pagrindą vertinti ne vien tai, ar modelyje numatyti atsparumą stiprinantys elementai, bet ir tai, kokiais rodikliais ateityje galėtų būti tikrinamas atsparumo pokytis modelį taikant praktikoje. E. sveikatos sistemos kibernetinio atsparumo operacionalizavimo schema pateikiama 4 paveiksle.



4 pav. E. sveikatos sistemos kibernetinio atsparumo operacionalizavimo schema

Šaltinis: sudaryta autorės, remiantis Linkov ir kt. (2013), Francis ir Bekera (2014), Coventry ir Branley (2018), Jalali ir Kaiser (2018), Garcia-Perez ir kt. (2023), Dupont ir kt. (2023)

4 paveiksle pateikta schema parodo loginį perėjimą nuo kibernetinio saugumo valdymo modelio reikalavimų prie empiriškai vertinamų kibernetinio atsparumo rodiklių. Pirmiausia modelio funkciniai ir nefunkciniai reikalavimai sudaro pagrindą atsparumo vertinimui, nes jie apima rizikų valdymą, incidentų valdymą, prieigos valdymą, duomenų apsaugą, veiklos tęstinumą, atitiktį teisės aktams, sąveikumą, patikimumą, organizacinę brandą ir organizacinį atsparumą. Šie reikalavimai operacionalizuojami per septynias atsparumo dimensijas: pasirengimą, aptikimą, reagavimą, atkūrimą, paslaugų tęstinumą, mokymąsi ir prisitaikymą bei organizacinę brandą.

Kiekviena dimensija siejama su konkrečiomis operacinių rodiklių grupėmis. Laiko rodikliai leidžia vertinti, kaip greitai organizacija aptinka incidentus, reaguoja į juos ir atkuria paslaugas. Procesų rodikliai parodo, ar organizacijoje veikia rizikų vertinimo, veiklos tęstinumo, atkūrimo, incidentų registravimo ir pratybų mechanizmai. Rezultatų rodikliai leidžia vertinti praktinį atsparumo pasireiškimą, pavyzdžiui, kritinių paslaugų prieinamumą, neplanuotų sutrikimų trukmę, atsarginių kopijų testų rezultatus ir korekcinių veiksmų įgyvendinimą. Brandos ir valdymo rodikliai atskleidžia, ar atsparumas yra integruotas į organizacijos valdymo struktūras, atsakomybes, vadovybės peržiūras, biudžeto planavimą ir tiekėjų saugumo vertinimą.

Tokia operacionalizavimo logika leidžia kibernetinį atsparumą vertinti ne vien normatyviai, bet ir empiriškai. Atsparumo pokytis galėtų būti nustatomas lyginant pasirinktų rodiklių reikšmes prieš modelio taikymą ir po jo taikymo, pavyzdžiui, vertinant incidentų aptikimo laiką, reagavimo laiką, paslaugų atkūrimo trukmę, kritinių paslaugų prieinamumą, incidentų registravimo pilnumą, atsarginių kopijų testavimo rezultatus, korekcinių veiksmų įgyvendinimą ir brandos vertinimo pokyčius.

2.2.2. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui pritaikomumo principai

Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui praktinė vertė atsiskleidžia tik tada, kai jis gali būti taikomas skirtingo dydžio, brandos, technologinės pažangos ir organizacinės struktūros sveikatos sektoriaus institucijose. Todėl mokslinėje literatūroje vis dažniau akcentuojamas modelio pritaikomumas, suprantamas kaip gebėjimas veikti realioje institucinėje aplinkoje, išlaikant teorinį nuoseklumą ir metodologinį pagrįstumą (Aven, 2016; Podrecca ir kt., 2025).

Remiantis 2.2.1 poskyryje išskirtais funkciniais ir nefunkciniais reikalavimais bei jiems priskirtais empiriniais indikatoriais, modelio pritaikomumas šiame tyrime traktuojamas kaip daugiamatis konstruktas, apimantis technologinius, organizacinius, procesinius ir valdymo aspektus. Toks požiūris leidžia išvengti siauro kibernetinio saugumo supratimo, kai modelio veiksmingumas vertinamas tik pagal techninių kontrolės priemonių diegimą, neatsižvelgiant į jų sąveiką su organizaciniais procesais, darbuotojų elgsena ir valdymo kultūra (Bada ir Nurse, 2019).

Sveikatos sektorius pasižymi dideliu instituciniu heterogeniškumu – nuo nacionalinių e. sveikatos platformų iki lokalių sveikatos priežiūros įstaigų informacinių sistemų (Sittig ir Singh, 2016). Organizacijos skiriasi dydžiu, technologine branda,

personalo kompetencijomis ir priklausomybe nuo išorinių paslaugų teikėjų. Todėl kibernetinio saugumo valdymo modelis neturėtų būti formuluojamas kaip vienodas kontrolės priemonių rinkinys visoms organizacijoms. Jis turi veikti kaip lanksti valdymo struktūra, leidžianti įsivertinti pradinę būklę, nustatyti prioritetines rizikas ir pasirinkti proporcingas saugumo stiprinimo priemones (Burke ir kt., 2024; O'Brien ir kt., 2024).

Modelio praktinis pritaikomumas taip pat priklauso nuo to, ar jame numatomi aiškūs prioritetizavimo ir tobulinimo ciklai. Tyrimai rodo, kad sveikatos priežiūros organizacijos dažnai susiduria su ribotų išteklių, kompetencijų stokos ir nepakankamos institucinės paramos problema (Hasegawa ir kt., 2024). Nors šio darbo kontekstas yra Lietuvos e. sveikatos sistema, ši įžvalga metodologiškai svarbi, nes parodo, kad modelis turi būti ne tik teoriškai išsamus, bet ir praktiškai įgyvendinamas skirtingose organizacijose. Tai leidžia modelį naudoti tiek strateginiam planavimui, tiek operaciniam saugumo valdymui, pritaikant jo komponentus pagal institucijos dydį, funkcijas ir turimus išteklius (Radanliev ir kt., 2019).

Vienas svarbiausių pritaikomumo principų yra brandos orientacija, leidžianti kibernetinio saugumo valdymą vertinti kaip laipsnišką ir nuoseklų procesą. Brandos principais grindžiami modeliai padeda organizacijoms nustatyti esamą būklę, apibrėžti realistiškus tobulinimo tikslus ir planuoti pažangą ilgalaikėje perspektyvoje (Suorsa, 2023). Mokslinėje literatūroje pabrėžiama, kad brandos logika sudaro sąlygas pereiti nuo formalaus atitikties užtikrinimo prie realaus organizacinio atsparumo stiprinimo (Puhakainen ir Siponen, 2010). Šis principas tiesiogiai siejasi su 2.2.1 poskyryje pateiktais empiriniais indikatoriais, kurie leidžia fiksuoti ne tik kontrolės priemones, bet ir jų veiksmingumą skirtinguose brandos etapuose.

Ne mažiau reikšmingas yra integruojamumo principas, pagal kurį kibernetinio saugumo valdymo modelis turi būti suderintas su kitomis organizacijos valdymo sistemomis. Izoliuoti saugumo modeliai dažnai tampa fragmentuoti ir praranda strateginę reikšmę, jeigu nėra susieti su rizikų valdymu, veiklos tęstinumo planavimu ar bendruoju strateginiu valdymu (Ransbotham ir kt., 2012). E. sveikatos sistemų atveju šis aspektas ypač svarbus, nes informacinės sistemos tiesiogiai susijusios su klinikiniais procesais, pacientų sauga ir paslaugų kokybe (Kruse ir kt., 2017).

Modelio pritaikomumas taip pat priklauso nuo matomumo ir atsekamumo principo. Šis principas leidžia susieti strateginius kibernetinio saugumo tikslus su konkrečiomis valdymo priemonėmis, atsakomybėmis ir rezultatais. Mokslinėje literatūroje pabrėžiama, kad saugumo iniciatyvos tampa veiksmingesnės tada, kai jų rezultatai yra išmatuojami ir suprantami sprendimų priėmėjams (Gordon ir kt., 2016). 2.2.1 poskyryje pateikti indikatoriai sudaro prielaidas kurti aiškią sąsają tarp politikų, procedūrų, technologinių sprendimų ir jų poveikio organizacijos atsparumui. Tai ypač svarbu rengiant empirinį tyrimą, kuriame vertinamas modelio tinkamumas, praktinis pritaikomumas ir tobulinimo kryptys.

Svarbus pritaikomumo aspektas yra ir organizacinis priimtinumas, apimantis darbuotojų įtrauktį, atsakomybių aiškumą ir sprendimų suprantamumą. Empiriniai tyrimai rodo, kad dalis kibernetinio saugumo iniciatyvų žlunga ne dėl technologinių

apribojimų, bet dėl organizacinio pasipriešinimo, nepakankamo darbuotojų įsitraukimo ar riboto supratimo apie saugumo priemonių naudą (Herath ir Rao, 2009; Bulgurcu ir kt., 2010). Todėl modelio struktūra turi būti orientuota ne tik į kontrolę, bet ir į organizacinį mokymąsi, saugumo kultūros formavimą ir aiškų atsakomybių paskirstymą.

Papildomą reikšmę modelio pritaikomumui suteikia reguliacinis lankstumas. Sveikatos sektorius veikia griežtai reguliuojamoje aplinkoje, kurioje kibernetinio saugumo reikalavimai nuolat kinta ir griežtėja. Tyrimai pabrėžia, kad lankstūs valdymo modeliai, gebantys prisitaikyti prie naujų teisinių ir standartizavimo reikalavimų, yra tvaresni ir mažiau pažeidžiami ilgalaikėje perspektyvoje (Bamberger ir Mulligan, 2011). Tai leidžia modelį naudoti ne tik esamai būklei vertinti, bet ir kaip adaptacinį instrumentą būsimiems reguliaciniams ir technologiniams pokyčiams valdyti.

Apibendrinant galima teigti, kad modelio pritaikomumo principai sudaro jungiamąją grandį tarp 2.2.1 poskyryje išskirtų reikalavimų ir praktinio kibernetinio saugumo valdymo modelio kūrimo. Branda, integruojamumas, matomumas, atsekamumas, organizacinis priimtinumas ir reguliacinis lankstumas leidžia modelį transformuoti iš teorinės konstrukcijos į praktinį valdymo instrumentą. Šių principų identifikavimas sudaro metodologinį pagrindą tolesnei kibernetinio saugumo valdymo modelio prielaidų, valdymo lygių ir struktūrinių sprendimų analizei, kuri plėtojama 2.3 skyriuje.

2.2.3. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui struktūros komponentų identifikavimas

Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui struktūros komponentų identifikavimas yra esminis etapas, leidžiantis pereiti nuo abstrakčių principų ir reikalavimų prie aiškiai apibrėžtos, praktiškai taikomos valdymo architektūros. Modeliai, kuriuose struktūriniai elementai nėra aiškiai identifikuoti ir tarpusavyje susieti, dažnai lieka deklaratyvūs ir sunkiai pritaikomi organizacinėje praktikoje (Aven, 2016; Suorsa, 2024). Todėl šiame poskyryje siekiama sistemingai išskirti pagrindinius kibernetinio saugumo valdymo modelio komponentus, kurie yra būtini e. sveikatos sistemų tobulinimui.

Remiantis ankstesniuose poskyriuose išnagrinėtais funkciniais ir nefunkciniais reikalavimais, taip pat teorinių ir praktinių valdymo modelių analize, struktūros komponentai suprantami kaip tarpusavyje sąveikaujantys elementai, apimantys strateginį, organizacinį, procesinį ir technologinį lygmenis. Būtent tokia daugiasluoksnė struktūra leidžia efektyviausiai valdyti sudėtingas sistemas, būdingas e. sveikatos aplinkai (Sittig ir Singh, 2016; Radanliev ir kt., 2019).

Vienas fundamentalių struktūros komponentų yra strateginio valdymo lygmuo, kuriame apibrėžiami kibernetinio saugumo tikslai, prioritetai ir jų sąsajos su organizacijos misija bei veiklos rezultatais. Be aiškios strateginės krypties kibernetinis saugumas organizacijose tampa fragmentuotas ir reaguojantis, o ne sistemiškai valdomas (Gordon ir kt., 2016). E. sveikatos sistemų kontekste strateginis komponentas taip pat apima suderinamumą su nacionalinėmis ir tarptautinėmis reguliavimo nuostatomis,

kurios daro tiesioginę įtaką saugumo valdymo architektūrai.

Kitas esminis komponentas yra valdymo ir atsakomybių struktūra, apimanti aiškų vaidmenų, funkcijų ir sprendimų priėmimo mechanizmų paskirstymą. Literatūroje pabrėžiama, kad neapibrėžtos atsakomybės yra viena dažniausių kibernetinio saugumo spragų priežasčių, ypač didelėse, tarpinstitucinėse sistemose (Herath ir Rao, 2009; Bada ir Nurse, 2019). E. sveikatos sistemose šis komponentas yra svarbus dėl sudėtingos suinteresuotųjų šalių struktūros, apimančios sveikatos priežiūros įstaigas, valstybines institucijas, informacinių technologijų paslaugų teikėjus ir duomenų tvarkytojus.

Trečiasis struktūrinis komponentas yra rizikų ir kontrolės procesų blokas, kuriame integruojami rizikų identifikavimo, vertinimo, valdymo ir stebėsenos mechanizmai. Efektyvūs kibernetinio saugumo modeliai pasižymi nuolatiniu grįžtamuoju ryšiu tarp rizikos vertinimo rezultatų ir taikomų kontrolės priemonių (Podrecca ir kt., 2025). E. sveikatos sistemų atveju šis komponentas turi apimti ne tik technologines rizikas, bet ir klinikinių procesų, duomenų vientisumo bei paslaugų tęstinumo aspektus.

Neatsiejama struktūros dalis yra incidentų valdymo ir organizacinio atsparumo komponentas. Organizacijos, kurios incidentų valdymą integruoja į bendrą valdymo struktūrą, pasižymi didesniu atsparumu ir greitesniu veiklos atstatymu (Ransbotham ir kt., 2012). E. sveikatos sektoriuje šis komponentas tiesiogiai siejamas su pacientų sauga ir paslaugų tęstinumu, todėl jo reikšmė yra kritinė.

Papildomą struktūrinę dimensiją sudaro žmogiškųjų ir organizacinių gebėjimų komponentas, apimantis kompetencijų ugdymą, saugumo kultūrą ir darbuotojų elgsenos valdymą. Empiriniai tyrimai nuosekliai rodo, kad net pažangiausios technologinės priemonės praranda efektyvumą, jei nėra palaikomos tinkamais organizaciniais gebėjimais ir darbuotojų sąmoningumu (Puhakainen ir Siponen, 2010; Bulgurcu ir kt., 2010). E. sveikatos sistemose šis aspektas yra ypač aktualus dėl klinikinio darbo specifikos ir didelio darbo tempo.

Galiausiai, struktūros komponentų identifikavimas apima ir technologinės infrastruktūros bei sąveikumo komponentą, kuris užtikrina, kad saugumo sprendimai būtų integruoti į esamą e. sveikatos sistemų architektūrą. Fragmentuoti ar izoliuoti techniniai sprendimai dažnai sukuria naujas rizikas vietoj to, kad jas sumažintų (Kruse ir kt., 2017). Todėl technologinis komponentas turi būti vertinamas kaip integrali valdymo modelio dalis, o ne savarankiškas elementas.

Apibendrinant galima teigti, kad kibernetinio saugumo valdymo modelio struktūros komponentų identifikavimas leidžia suformuoti nuoseklią, tarpusavyje suderintą architektūrą, apimančią strateginius, organizacinius, procesinius, žmogiškuosius ir technologinius aspektus. Šių komponentų tarpusavio sąveika sudaro prielaidas kurti integruotą valdymo modelį, kuris gali būti adaptuotas e. sveikatos sistemų specifikai ir vėliau empiriškai vertinamas. Identifikuoti struktūros komponentai tampa atspirties tašku kitame disertacijos poskyryje, kuriame nagrinėjami valdymo lygiai, hierarchija ir informacijos srautų organizavimas kuriamame kibernetinio saugumo valdymo modelyje.

Analizė parodė, jog modelio tvarumas ir pritaikomumas priklauso nuo jo gebėjimo integruoti rizikų valdymą, incidentų reagavimo mechanizmus, atsakomybių

paskirstymą bei vertinamus brandos indikatorius. Tokia struktūruota prieiga sudaro prielaidas nuosekliai identifikuoti esminius valdymo komponentus ir užtikrina metodologinį pagrindą tolesniam modelio architektūros formavimui, kuris detalizuojamas 2.3. disertacijos skyriuje.

2.3. Prielaidos kibernetinio saugumo valdymo modeliui e. sveikatos sistemos tobulinimui kurti

Kibernetinio saugumo valdymo modelio konstravimas e. sveikatos sistemos tobulinimo tikslams reikalauja aiškiai apibrėžtų prielaidų, kurios leistų nuosekliai pereiti nuo normatyvinių reikalavimų ir gerųjų praktikų prie struktūriškai aprašomo, empiriškai pamatuojamo ir instituciniu požiūriu įgyvendinamo modelio. Informacijos saugumo ir kibernetinio saugumo tyrimuose vis dažniau pabrėžiama, kad organizacijų saugumo problemos yra socio-techninės ir valdymo pobūdžio, kylančios iš technologijų, procesų, atsakomybių, sprendimų priėmimo ir žmonių elgsenos sąveikos (Sittig ir Singh, 2016; Dhillon ir Backhouse, 2001). Ši prielaida ypač svarbi e. sveikatos ekosistemose, kur informacinės sistemos yra tiesiogiai susietos su pacientų sauga, todėl net trumpalaikiai sutrikimai ar klaidos turi neproporcingai didelį poveikį veiklai (Sittig ir Singh, 2016; Alhuwail ir kt., 2021).

Kitas svarbus teorinis atspirties taškas – kibernetinį saugumą vertinti kaip organizacinį gebėjimą valdyti riziką, o ne kaip izoliuotų kontrolės priemonių rinkinį. Veiksmingas valdymas prasideda nuo aiškaus rizikos sampratos suvienodinimo, sprendimų kriterijų ir priimtinumo ribų apibrėžimo, o tai leidžia nuosekliai susieti grėsmes su valdymo priemonėmis ir jų prioritetais (Aven, 2016). Organizacinių sprendimų kontekste tai reiškia, kad modelio struktūra turi iš anksto numatyti, kaip bus atliekamas rizikų identifikavimas ir vertinimas, kaip bus pasirenkamos kontrolės priemonės, kaip bus matuojamas jų veiksmingumas ir kaip rezultatai grįžtamai koreguos valdymo sprendimus (Podrecca ir kt., 2025). Toks grįžtamojo ryšio principas atitinka šiuolaikinę informacinių sistemų tyrimų logiką, kurioje kibernetinis saugumas traktuojamas kaip nuolat tobulinama valdymo funkcija, o ne vienkartinis projektas (Ransbotham ir kt., 2012).

E. sveikatos kontekste prielaidų svarbą dar labiau sustiprina tai, kad organizacijų gebėjimas įgyvendinti saugumo reikalavimus priklauso nuo valdymo ir elgsenos veiksnių. Politikų ir procedūrų buvimas savaime negarantuoja jų laikymosi, o darbuotojų elgsena, suvokimas ir organizacinė kultūra tampa kritiniais kintamaisiais, lemiančiais realų saugumo lygį (Bulgurcu ir kt., 2010; Herath ir Rao, 2009). Sveikatos sektoriuje šie aspektai ypač aktualūs dėl aukšto darbo tempo, prioritetų, orientuotų į klinikinius rezultatus, ir dažnai nevienodo informacinio raštingumo, tai paaiškina, kodėl modelyje būtina iš anksto numatyti kompetencijų valdymo, mokymų ir sąmoningumo stiprinimo komponentus kaip struktūrinę, o ne papildomą priemonę (Alhuwail ir kt., 2021; Mikuletič ir kt., 2024).

Dar viena svarbi prielaida yra ta, kad e. sveikatos kibernetinio saugumo valdymas peržengia vienos organizacijos ribas. Tarpinstitucinis sąveikumas, bendri registrai, integracinės sąsajos ir išoriniai tiekėjai lemia, kad saugumo sprendimai turi būti

koordinuojami ekosistemos lygmeniu, o rizikos gali plisti per tiekimo grandines ir sistemų integracijas (Bada ir Nurse, 2019). Todėl modelio architektūra turi aiškiai apibrėžti atsakomybių paskirstymą, sprendimų eskalavimo taisykles ir bendrus minimalius saugumo reikalavimus visiems ekosistemos dalyviams. Priešingu atveju visos sistemos atsparumas priklausys nuo silpniausios grandies.

Metodologiškai svarbi prielaida yra modelio patikrinamumas, jis turi būti sukonstruotas taip, kad būtų įmanoma empiriškai įvertinti jo taikymo būklę ir pokytį. Informacinių sistemų tyrimuose plačiai taikoma *artefakto* kūrimo ir vertinimo logika, kurioje modelis laikomas tyrimo rezultatu, o jo kokybė grindžiama aiškiais konstruktais, matavimo rodikliais ir validavimo procedūromis (Hevner ir kt., 2004). Dėl to šiame skyriuje prielaidos formuluojamos taip, kad jos tiesiogiai remtųsi ankstesniame poskyryje parengta reikalavimų – indikatorių struktūra ir sudarytų aiškias nuorodas į 3 skyriaus empirinius tyrimus.

Atsižvelgiant į šias nuostatas, toliau sistemingai detalizuojamos prielaidos, kurios leidžia sukonstruoti nuoseklią valdymo modelio architektūrą: (I) valdymo lygiai ir hierarchija, užtikrinantys sprendimų priėmimo logiką ir atsakomybės „vertikalę“; (II) informacijos srautų saugumas, apimantis duomenų judėjimo kontrolę, atsekamumą ir praktinę stebėseną; (III) atsakomybės pasiskirstymas, kuris mažina sprendimų neapibrėžtumą incidentų ir rizikų valdymo situacijose; ir (IV) modelio teorinis aprašymas, leidžiantis aiškiai atvaizduoti sąsajas tarp komponentų.

2.3.1. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui valdymo lygiai ir hierarchija

Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui struktūroje valdymo lygių ir hierarchijos apibrėžimas yra būtina prielaida, leidžianti sistemiškai susieti strateginius sprendimus, organizacinius procesus ir operacinį saugumo užtikrinimą. Viena dažniausių kibernetinio saugumo valdymo nesėkmių priežasčių yra aiškios hierarchinės struktūros ir atsakomybių paskirstymo stoka (Weill ir Ross, 2004; Von Solms, 2006). Tai ypač aktualu e. sveikatos sistemose, kuriose sprendimų priėmimas vyksta keliuose organizaciniuose, technologiniuose ir tarpinstitucinės sąveikos lygmenyse.

E. sveikatos sistemos kibernetinio saugumo valdysena negali būti siejama vien su informacinių technologijų specialistų atsakomybe. Skaitmeninės transformacijos sąlygomis kibernetinis saugumas turi būti siejamas su darbuotojų elgsena, vadovybės įsipareigojimu, rizikų komunikacija ir organizacine kultūra (Alharbi ir Alkhalifah, 2025). Todėl modelyje būtina aiškiai atskirti strateginį, taktinį, operacinį ir technologinį valdymo lygmenis, kartu numatant jų tarpusavio sąveikos mechanizmus.

Valdymo hierarchija šiame tyrime suprantama kaip formalizuota sprendimų priėmimo, atsakomybių ir kontrolės santykių sistema, leidžianti koordinuoti kibernetinio saugumo veiklas skirtinguose organizacijos sluoksniuose. Tokia hierarchija užtikrina, kad strateginiai tikslai būtų nuosekliai perkeliami į taktinius planus, operacines procedūras ir technologines kontrolės priemones, o grįžtamasis ryšys iš žemesnių lygmenų

būtų naudojamas valdymo sprendimams koreguoti (De Haes ir Van Grembergen, 2015, Hagen ir kt., 2011).

Papildomą reikšmę valdysenos struktūrai suteikia trečiųjų šalių ir verslo partnerių įsitraukimas. Sveikatos sektoriuje organizacijų pažeidžiamumas gali būti susijęs ne tik su jų pačių informacinėmis sistemomis, bet ir su išorinių paslaugų teikėjų, duomenų tvarkytojų ar kitų partnerių saugumo spragomis. Išpirkos reikalaujančių atakų analizė rodo, kad tiekimo grandinės ir partnerių pažeidžiamumai gali turėti reikšmingą poveikį sveikatos organizacijų veiklai (Cornejo, 2026). Todėl e. sveikatos kibernetinio saugumo modelis turi apimti ne tik vidinius procesus, bet ir tiekimo grandinės, paslaugų teikėjų bei tarpinstitucinių priklausomybių valdymą.

Strateginis kibernetinio saugumo valdymo lygmuo apima aukščiausio lygio sprendimus, susijusius su organizacijos saugumo vizija, ilgalaikiais tikslais, prioritetais ir rizikos tolerancijos ribomis. Organizacijos, kuriose kibernetinis saugumas įtraukiamas į strateginę darbotvarkę, pasižymi didesniu atsparumu ir geresniu gebėjimu valdyti sistemines rizikas (Kwon ir Johnson, 2014). E. sveikatos sistemų kontekste šis lygmuo įgyja papildomą reikšmę, nes saugumo sprendimai yra susiję ne tik su informacinių sistemų apsauga, bet ir su visuomenės sveikata, pacientų pasitikėjimu, valstybės institucijų reputacija ir ilgalaikėmis skaitmeninės transformacijos kryptimis. Strateginis saugumo valdymas turi apimti ne tik atitiktį reguliaciniams reikalavimams, bet ir investicinius sprendimus, žmogiškųjų išteklių politiką bei tarporganizacinį bendradarbiavimą (Bada ir Nurse, 2019). Didelio masto skaitmeninių sistemų valdymui svarbus tarpinstitucinis bendradarbiavimas, efektyvi komunikacija, išteklių koordinavimas ir gebėjimas prisitaikyti prie skirtingų suinteresuotųjų šalių poreikių (Limba ir kt., 2025).

Taktinis valdymo lygmuo veikia kaip tarpinė grandis tarp strateginių sprendimų ir jų praktinio įgyvendinimo. Šiame lygmenyje strateginės nuostatos transformuojamos į politikas, procedūras, standartus, planus ir koordinavimo mechanizmus. Šiame lygmenyje dažnai kyla koordinavimo problemų, kai strateginiai tikslai nėra tinkamai perkeliami į praktinius veiksmus (Puhakainen ir Siponen, 2010). E. sveikatos sistemose taktinis lygmuo apima informacijos saugumo vadovų, informacinių technologijų padalinių, klinikinių padalinių vadovų ir rizikos valdymo funkcijų sąveiką. Jo veiksmingumas priklauso nuo aiškiai apibrėžtų vaidmenų, formalizuotų sprendimų priėmimo procesų ir nuolatinės komunikacijos tarp padalinių (Herath ir Rao, 2009). Šiame lygmenyje taip pat formuojamos incidentų valdymo procedūros, mokymų programos, vidaus kontrolės mechanizmai ir rizikų valdymo priemonės.

Operacinis lygmuo apima kasdienę kibernetinio saugumo priemonių įgyvendinimo praktiką: techninių kontrolės priemonių taikymą, sistemų stebėseną, incidentų registravimą, pirminį reagavimą ir naudotojų veiksmus. Tyrimai rodo, kad net ir tinkamai suformuluotos strategijos praranda veiksmingumą, jeigu operaciniame lygmenyje trūksta kompetencijų, išteklių ar aiškių procedūrų (Dhillon ir Backhouse, 2001). Sveikatos sektoriuje šis lygmuo pasižymi specifiniais iššūkiais dėl nepertraukiamo sistemų veikimo poreikio. Medicinos personalas dažnai turi derinti saugumo reikalavimus su skubiais klinikiniais sprendimais, o tai didina klaidų tikimybę (Ashenden ir Lawrence, 2016). Todėl operacinio lygmens valdymas turi būti glaudžiai susietas su taktiniu

lygmeniu, kad saugumo priemonės būtų praktiškai įgyvendinamos ir neprieštarautų sveikatos paslaugų teikimo logikai.

Technologinis lygmuo apima informacines sistemas, infrastruktūrą, technines kontrolės priemones, prieigos valdymo sprendimus, stebėsenos sistemas, atsargines kopijas, medicininius įrenginius ir integracines sąsajas. Nors technologinis lygmuo dažnai laikomas pagrindine kibernetinio saugumo įgyvendinimo erdve, jis negali būti atskirtas nuo strateginių, taktinių ir operacinių sprendimų. Technologinės priemonės yra veiksmingos tik tada, kai jos atitinka organizacijos rizikos prioritetus, yra palaikomos aiškiomis procedūromis ir integruotos į bendrą saugumo valdysenos sistemą.

Kibernetinio saugumo valdymo hierarchija neturėtų būti suprantama vien kaip griežta vertikali struktūra. Veiksmingas valdymas reikalauja ir horizontaliosios koordinacijos tarp skirtingų funkcinių sričių, padalinių, institucijų ir išorinių partnerių (De Haes ir Van Grembergen, 2015). E. sveikatos sistemose tai ypač svarbu dėl tarpinstitucinių duomenų mainų, bendrų infrastruktūrų naudojimo ir priklausomybės nuo išorinių paslaugų teikėjų. Tyrimai rodo, kad organizacijos, gebančios derinti vertikalią atsakomybių hierarchiją su horizontalia bendradarbiavimo struktūra, pasižymi didesniu organizaciniu atsparumu ir greitesniu reagavimu į incidentus (Boyson, 2014).

Todėl šiame disertaciniame modelyje daroma prielaida, kad valdymo lygmenys turi būti aiškiai atskirti, tačiau tarpusavyje susieti formaliais ir neformaliais koordinavimo mechanizmais. Vertikali valdymo logika leidžia užtikrinti sprendimų nuoseklumą nuo strateginių tikslų iki operacinio įgyvendinimo, o horizontalioji koordinacija sudaro sąlygas suderinti skirtingų padalinių, institucijų ir partnerių veiksmus. Toks derinys ypač svarbus e. sveikatos sistemose, kuriose kibernetinio saugumo valdymas peržengia vienos organizacijos ribas.

Valdymo lygių ir hierarchijos analizė sudaro pagrindą kibernetinio saugumo valdymo modelio struktūriniam projektavimui. Aiškiai apibrėžti lygmenys leidžia susieti modelio komponentus su konkrečiomis organizacinėmis funkcijomis ir vėliau juos operacionalizuoti empirinio tyrimo metu. Moksliniuose tyrimuose pabrėžiama, kad toks struktūrinis aiškumas leidžia pereiti nuo abstrakčių saugumo koncepcijų prie praktiškai vertinamų modelių (Ransbotham ir kt., 2012).

Apibendrinant galima teigti, kad valdymo lygių ir hierarchijos įtvirtinimas yra būtina sąlyga kuriant e. sveikatos sistemų sudėtingumui pritaikytą kibernetinio saugumo valdymo modelį. Strateginio, taktinio, operacinio ir technologinio lygmenų sąveika, papildyta vertikalios ir horizontalios koordinacijos principais, leidžia nuosekliai paskirstyti atsakomybes, susieti sprendimus su praktiniu įgyvendinimu ir užtikrinti grįžtamąjį ryšį modelio tikslinimui. Ši analizė nukreipia į tolesnį informacijos srautų saugumo ir atsakomybių paskirstymo nagrinėjimą kituose šio skyriaus poskyriuose.

2.3.2. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui informacijos srautų saugumas

Informacijos srautų saugumas yra viena iš esminių prielaidų veiksmingam kibernetinio saugumo valdymo modeliui e. sveikatos sistemose kurti. Informacijos srautų

saugumas apima visą duomenų gyvavimo ciklą, nuo jų sukūrimo ir apdorojimo iki perdavimo, saugojimo ir sunaikinimo, bei sąveiką tarp technologinių, organizacinių ir žmogiškųjų elementų (von Solms ir van Niekerk, 2013). Būtent informacijos srautų valdymas leidžia identifikuoti kritinius sąlyčio taškus, kuriuose kyla didžiausia kibernetinių incidentų rizika (Siponen ir kt., 2014).

E. sveikatos sistemose informacijos srautai pasižymi išskirtiniu sudėtingumu dėl didelio dalyvių skaičiaus, specifinių informacinių sistemų ir nuolatinio duomenų judėjimo tarp skirtingų organizacinių bei institucinių ribų. Tyrimai rodo, kad tokiose sistemose kibernetinės rizikos dažnai kyla dėl nepakankamai koordinuotų informacijos srautų ir neaiškiai apibrėžtų atsakomybių (Sittig ir Singh, 2016; Radanliev ir kt., 2019). Todėl informacijos srautų saugumas turi būti analizuojamas kaip integrali kibernetinio saugumo valdymo modelio dalis, o ne kaip atskira funkcija.

Vienas pagrindinių informacijos srautų saugumo aspektų yra duomenų judėjimo skaidrumas ir atsekamumas. Organizacijos, kurios neturi aiškaus supratimo apie tai, kur, kaip ir kokiais tikslais duomenys juda tarp sistemų ir procesų, susiduria su padidėjusia neteisėtos prieigos, duomenų nutekinimo ar netyčinio duomenų praradimo rizika (Singer ir Friedman, 2014; Tikkinen-Piri ir kt., 2018). E. sveikatos sistemose ši problema dar labiau paaštrėja dėl jautraus tvarkomų duomenų pobūdžio ir griežtų teisinio reguliavimo reikalavimų.

Kitas svarbus informacijos srautų saugumo elementas yra duomenų perdavimo kanalų apsauga. Didelė dalis kibernetinių incidentų yra susiję su nepakankamai apsaugotais sąsajų taškais tarp skirtingų informacinių sistemų, ypač tais atvejais, kai naudojamos trečiųjų šalių platformos ar debesų kompiuterijos sprendimai (Alsubaei ir kt., 2017). E. sveikatos sistemose tai apima duomenų mainus tarp gydymo įstaigų, laboratorijų, draudimo institucijų ir valstybinių registrų, todėl informacijos srautų saugumas tampa organizaciniu iššūkiu.

Organizaciniu lygmeniu informacijos srautų saugumas yra glaudžiai susijęs su procesų formalizavimu ir atsakomybės paskirstymu. Aiškiai apibrėžti informacijos srautai ir jų valdymo taisyklės leidžia sumažinti žmogiškųjų klaidų tikimybę ir užtikrinti nuoseklų saugumo priemonių taikymą visoje organizacijoje (Dhillon ir Backhouse, 2001; Ashenden ir Lawrence, 2016). Priešingai, neformalūs ar nepakankamai dokumentuoti informacijos srautai dažnai tampa aklomis zonomis, kuriose saugumo kontrolės neveikia arba veikia fragmentiškai.

Svarbu pažymėti, kad informacijos srautų saugumas e. sveikatos sistemose turi būti vertinamas ne tik vidinių organizacijos procesų, bet ir platesnės ekosistemos kontekste. Tarpinstituciniai informacijos srautai gali sukurti sistemines rizikas, kai vienos organizacijos saugumo spragos daro poveikį visai paslaugų teikimo grandinei (Bada ir Nurse, 2019; Boyson, 2014). Todėl veiksmingas informacijos srautų saugumo valdymas reikalauja koordinuotų sprendimų ir bendrų standartų taikymo tarp skirtingų suinteresuotųjų šalių.

Siekiant struktūruotai apibendrinti pagrindinius informacijos srautų saugumo aspektus ir jų sąsają su kibernetinio saugumo valdymo modelio kūrimu, toliau pateikiama analitinė 12 lentelė.

12 lentelė. Informacijos srautų saugumo dimensijos e. sveikatos sistemose ir jų empiriniai indikatoriai

Informacijos srautų dimensija	Aprašymas	Tipinės rizikos	Valdymo priemonės	Empiriniai indikatoriai
Duomenų srautų identifikavimas	Duomenų judėjimo tarp sistemų ir procesų apibrėžimas	Nežinomi duomenų srautai, nevaldomi sąsajų taškai	Duomenų srautų žemėlapiai, procesų dokumentavimas	Formalizuotų srautų dalis, identifikuotų sąsajų skaičius
Prieigos valdymas	Prieigos prie duomenų kontrolė skirtinguose srautų etapuose	Neautorizuota prieiga, privilegijų eskalacija	Rolėmis grįsta prieiga, autentifikavimo mechanizmai	Prieigos pažeidimų skaičius, peržiūrų reguliarumas
Duomenų perdavimo apsauga	Duomenų apsauga perdavimo metu	Duomenų perėmimas, modifikavimas	Šifravimas, saugūs protokolai	Šifruotų srautų dalis, incidentų skaičius
Atsekamumas ir stebėsena	Veiksmų registravimas ir stebėjimas	Incidentų neaptikimas, vėluojantis reagavimas	Žurnalų analizė, stebėsenos sistemos	Aptikimo laikas, audito išvados
Tarpinstitucinis sąveikumas	Duomenų mainai tarp organizacijų	Grandininiai pažeidimai, priklausomybė nuo partnerių	Sutartys, bendri standartai	Partnerių atitikties lygis, bendrų incidentų skaičius

Šaltinis: sudaryta autorės, remiantis Dhillon ir Backhouse (2001), Sittig ir Singh (2016), Singer ir Friedman (2014), Radanliev ir kt. (2019), Bada ir Nurse (2019)

Apibendrinant galima teigti, kad informacijos srautų saugumas yra kertinė kibernetinio saugumo valdymo modelio e. sveikatos sistemose prielaida. Informacijos srautų identifikavimas, jų apsauga ir nuoseklus valdymas leidžia sumažinti sistemines rizikas, kylančias dėl sudėtingų technologinių ir organizacinių sąveikų. Analitinėje 12 lentelėje išskirtos dimensijos ir empiriniai indikatoriai sudaro pagrindą tolesniam modelio kūrimui ir tiesiogiai siejasi su disertacijos empirinėje dalyje atliekamu kibernetinio saugumo brandos vertinimu. Ši analizė taip pat sudaro prielaidas pereiti prie atsakomybės pasiskirstymo nagrinėjimo, kuris plėtojamas kitame poskyryje.

2.3.3. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui atsakomybės pasiskirstymas

Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui veiksmingumas reikšmingai priklauso nuo aiškaus, formaliai apibrėžto ir institucišKai įtvirtinto atsakomybių paskirstymo. Mokslinėje literatūroje pabrėžiama, kad net ir technologiškai brandžiose organizacijose kibernetinio saugumo priemonės tampa mažiau veiksmingos, jeigu atsakomybės yra fragmentuotos, dubliuojamos arba neaiškiai priskirtos (Dhillon, 2007). E. sveikatos sistemų kontekste ši problema įgyja papildomą reikšmę dėl sudėtingos institucinės aplinkos, daugelio suinteresuotųjų šalių ir didelio asmens sveikatos duomenų tvarkymo masto.

Atsakomybių paskirstymas šiame tyrime suprantamas kaip formalizuota funkcijų, sprendimų priėmimo teisių, atskaitomybės ryšių ir kontrolės mechanizmų sistema, leidžianti užtikrinti, kad kibernetinio saugumo valdymas nebūtų paliekamas vien informacinių technologijų padaliniui ar pavieniams specialistams. Kibernetinis saugumas e. sveikatos sistemoje apima ne tik informacinių sistemų apsaugą, bet ir duomenų valdymą, klinikinių procesų tęstinumą, incidentų koordinavimą, tiekėjų kontrolę ir naudotojų elgseną. Todėl atsakomybės turi būti paskirstytos taip, kad kiekvienas valdymo lygmuo ir kiekviena dalyvaujanti organizacija aiškiai suprastų savo vaidmenį saugumo užtikrinimo procese.

Strateginiame lygmenyje atsakomybė siejama su aukščiausios vadovybės ir valdymo organų vaidmeniu. Šiame lygmenyje nustatomos kibernetinio saugumo kryptys, rizikos tolerancijos ribos, skiriami ištekliai ir kuriami atskaitomybės mechanizmai. Mokslinėje literatūroje pabrėžiama, kad kibernetinis saugumas turi būti integruotas į bendrą organizacijos valdyseną ir rizikų valdymo sistemą (von Solms ir van Niekerk, 2013). Organizacijose, kuriose aukščiausio lygmens vadovybė aktyviai dalyvauja kibernetinio saugumo klausimuose, saugumo iniciatyvos paprastai yra nuoseklesnės ir labiau suderintos su organizacijos tikslais (Tallon ir kt., 2014, Tzavara ir kt., 2024).

Taktiniame lygmenyje atsakomybės siejamos su strateginių sprendimų perkėlimu į konkrečias politikas, procedūras, standartus ir koordinavimo mechanizmus. Šiame lygmenyje svarbus informacijos saugumo vadovų, rizikų valdymo funkcijų, informacinių technologijų padalinių, klinikinių padalinių vadovų ir administracijos bendradarbiavimas. Taktinis lygmuo leidžia sumažinti atotrūkį tarp strateginių sprendimų ir praktinio jų įgyvendinimo, nes būtent čia formuojamos incidentų valdymo procedūros, prieigos teisių valdymo taisyklės, mokymų programos ir vidaus kontrolės priemonės (Kankanhalli ir kt., 2003). E. sveikatos sistemose šio lygmens reikšmė ypač didelė, nes saugumo sprendimai turi būti suderinami su klinikiniais, administraciniais ir technologiniais procesais.

Operaciniame lygmenyje atsakomybės susijusios su kasdieniu kibernetinio saugumo priemonių taikymu ir naudotojų elgsena. Tai apima prieigos teisių administravimą, incidentų stebėseną, reagavimą į saugumo įvykius, sistemų atnaujinimą, atsarginių kopijų tikrinimą ir saugaus darbo taisyklių laikymąsi. Operacinio lygmens darbuotojų vaidmuo dažnai nepakankamai įvertinamas, nors būtent šiame lygmenyje

dažnai atsiskleidžia žmogiškojo veiksnio, procedūrų nesilaikymo ar nepakankamo pasirengimo keliamos rizikos (Parsons ir kt., 2017). Todėl atsakomybių paskirstymas turi apimti ne tik formalius vadovų ar specialistų vaidmenis, bet ir aiškiai apibrėžtas pareigas visiems e. sveikatos sistemos naudotojams.

Atskiras atsakomybių paskirstymo aspektas yra tarpinstitucinis ir tiekimo grandinės valdymas. E. sveikatos sistemose duomenų tvarkymas ir paslaugų teikimas dažnai apima trečiąsias šalis, informacinių technologijų paslaugų teikėjus, debesijos paslaugų tiekėjus, medicinos įrangos gamintojus, laboratorijas, vaistines ir kitus partnerius. Neapibrėžtos atsakomybės tiekimo grandinėje yra viena iš sisteminių saugumo spragų priežasčių (Boyson, 2014). Todėl atsakomybės turi būti įtvirtintos ne tik organizacijos vidaus dokumentuose, bet ir sutartyse, duomenų tvarkymo susitarimuose ir bendrose saugumo procedūrose.

Atsakomybių aiškumas glaudžiai susijęs su atskaitomybe ir skaidrumu. Organizacijos, taikančios aiškius atskaitomybės mechanizmus, reguliarius auditus ir veiklos rodiklius, turi geresnes prielaidas identifikuoti silpnąsias vietas ir tobulinti kibernetinio saugumo valdymą (Power, 2007). E. sveikatos kontekste tai svarbu ne tik organizacijos vidaus valdymui, bet ir pacientų bei visuomenės pasitikėjimui skaitmeninėmis sveikatos paslaugomis. Jeigu nėra aišku, kas atsakingas už prieigos teisių suteikimą, duomenų mainų sąsajų saugumą, incidento eskalavimą ar paslaugų atkūrimą, net ir techniškai pažangios saugumo priemonės gali tapti nepakankamos.

Todėl kuriamame kibernetinio saugumo valdymo modelyje atsakomybių paskirstymas turi būti siejamas su keliais pagrindiniais principais. Pirma, kiekviena saugumo funkcija turi turėti aiškų atsakingą subjektą. Antra, sprendimų priėmimo teisės ir atskaitomybės ryšiai turi būti formalizuoti. Trečia, atsakomybės turi apimti ne tik organizacijos vidų, bet ir tarpinstitucinius ryšius bei tiekimo grandinę. Ketvirta, atsakomybių įgyvendinimas turi būti tikrinamas per auditus, incidentų analizę, brandos vertinimą ir kitus operacinius rodiklius. Tokia atsakomybių logika leidžia modelį susieti ne tik su valdymo struktūra, bet ir su praktiniu saugumo veiksmingumu.

Apibendrinant galima teigti, kad atsakomybių paskirstymas yra viena esminių prielaidų kuriant integruotą kibernetinio saugumo valdymo modelį e. sveikatos sistemoms. Aiškiai apibrėžtos strateginio, taktinio, operacinio ir tarpinstitucinio lygmenų atsakomybės sudaro pagrindą nuosekliam saugumo sprendimų įgyvendinimui, incidentų koordinavimui, atskaitomybei ir organizaciniam mokymuisi. Šios įžvalgos leidžia pereiti prie kito poskyrio, kuriame modelio elementai struktūriškai jungiami į pradinę kibernetinio saugumo valdymo schemą.

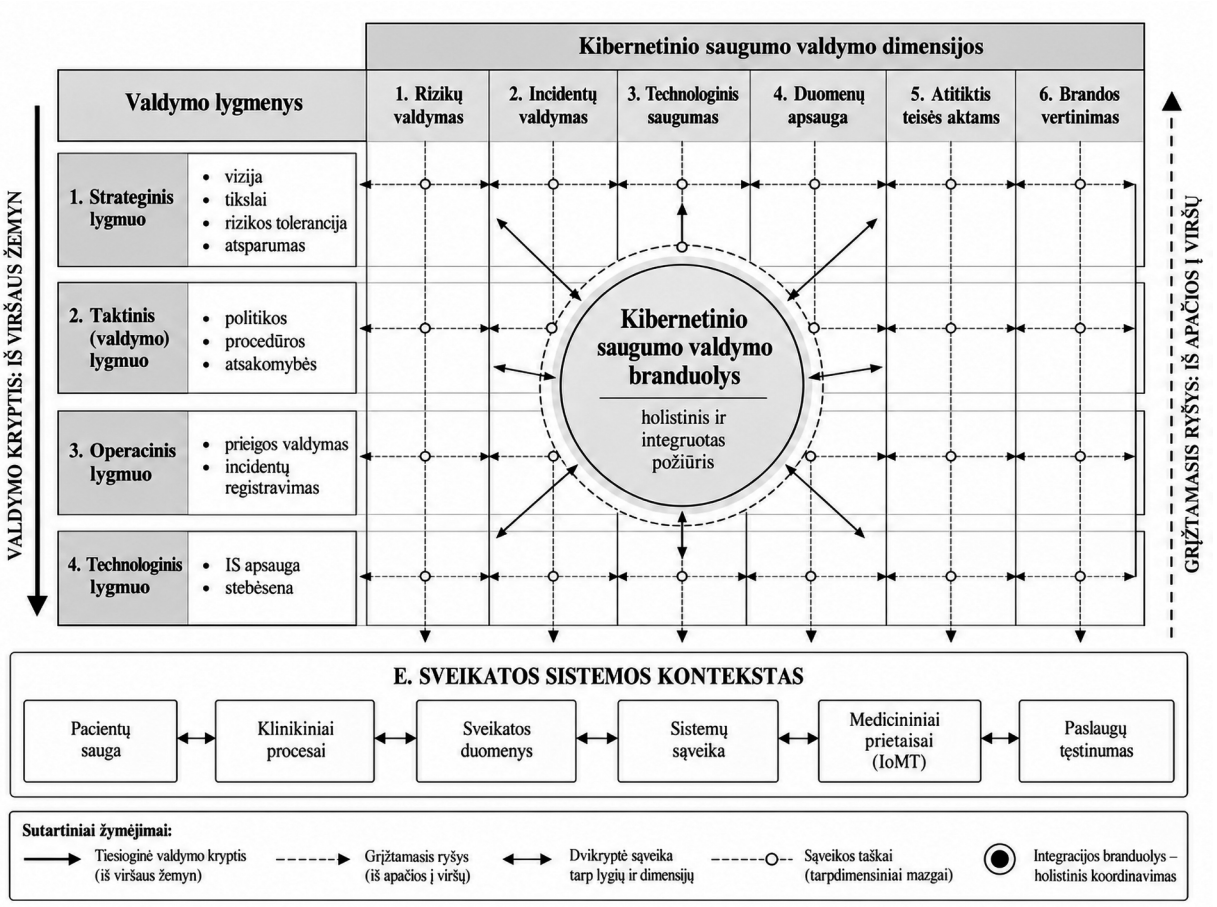
2.3.4. Koncepcinio kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui kūrimas

Siekiant konceptualiai apibendrinti ankstesniuose poskyriuose išanalizuotas kibernetinio saugumo valdymo prielaidas, teorinius modelius, tarptautinių standartų nuostatas bei e. sveikatos sistemos struktūrinius ypatumus, šiame poskyryje suformuojamas pradinis kibernetinio saugumo valdymo modelis, skirtas e. sveikatos

sistemos tobulinimui. Modelis kuriamas kaip teoriškai pagrįsta konceptuali struktūra, leidžianti sistemiškai atskleisti pagrindinius kibernetinio saugumo valdymo elementus, jų hierarchiją, funkcines dimensijas, sąveikos taškus ir ryšį su e. sveikatos sistemos specifika.

Pradinis modelis grindžiamas nuostata, kad kibernetinis saugumas e. sveikatos sistemose negali būti valdomas fragmentiškai ar apsiribojant pavienėmis techninėmis priemonėmis. Priešingai, jis turi būti suvokiamas kaip integruota valdymo sistema, apimanti strateginius sprendimus, organizacinius ir procesinius mechanizmus, technologinius sprendimus, duomenų apsaugą, atitiktį teisės aktams, brandos vertinimą ir nuolatinį grįžtamąjį ryšį. Tokia integruota perspektyva sudaro prielaidas kurti nuoseklų ir ilgalaikį kibernetinio saugumo valdymo pagrindą e. sveikatos sistemoje.

Modelis kuriamas kaip daugiamatė, hierarchinė ir tarp dalykinė schema, kurioje išskiriamos vertikaliosios valdymo ašys, horizontalieji valdymo lygmenys, per visus lygmenis einančios funkcinės dimensijos, centrinis kibernetinio saugumo valdymo branduolys ir e. sveikatos sistemos kontekstas. Tokia struktūra pasirinkta siekiant pabrėžti, kad kibernetinio saugumo valdymas apima ne atskiras funkcijas, bet tarpusavyje susijusių elementų visumą, kurios veiksmingumas priklauso nuo strateginių sprendimų, organizacinių procedūrų, operacinių veiksmų, technologinių priemonių ir nuolatinio vertinimo suderinamumo. Pradinis kibernetinio saugumo modelis pateikiamas 5 paveiksle.



5 pav. Koncepcinis kibernetinio saugumo valdymo modelis e. sveikatos sistemos tobulinimui

Šaltinis: sudaryta autorės

Kaip matyti 5 paveiksle, pradinis teorinis kibernetinio saugumo valdymo modelis e. sveikatos sistemos tobulinimui sudarytas iš kelių tarpusavyje susijusių struktūrinių elementų: vertikalios valdymo krypties, grįžtamojo ryšio ašies, keturių valdymo lygmenų, šešių funkcinių kibernetinio saugumo valdymo dimensijų, integruojančio kibernetinio saugumo valdymo branduolio ir e. sveikatos sistemos konteksto. Tokia modelio struktūra pasirinkta siekiant parodyti, kad kibernetinio saugumo valdymas e. sveikatos sistemoje negali būti suprantamas kaip pavienių techninių priemonių taikymas. Jis turi būti analizuojamas kaip koordinuota ir nuolat tobulinama valdymo sistema, apimanti strateginius sprendimus, organizacinius procesus, operacinę praktiką, technologines kontrolės priemones ir e. sveikatos sistemos veikimo ypatumus.

Pirmoji modelio dalis yra vertikalioji valdymo kryptis, žyminti sprendimų judėjimą iš viršaus žemyn. Ji parodo, kad kibernetinio saugumo valdymas pradedamas nuo strateginių sprendimų, kurie vėliau perkeliami į taktinius, operacinius ir technologinius veiksmus. Toks principas leidžia užtikrinti, kad kibernetinis saugumas būtų siejamas su bendraisiais e. sveikatos sistemos plėtros, paslaugų tęstinumo, pacientų saugos ir sveikatos duomenų apsaugos tikslais.

Antroji modelio dalis yra grįžtamojo ryšio ašis, žyminti informacijos judėjimą iš apačios į viršų. Ji rodo, kad technologiniame ir operaciniame lygmenyse fiksuojami saugumo įvykiai, incidentai, naudotojų elgsena, techninių priemonių veiksmingumas, duomenų apsaugos problemos ir paslaugų sutrikimai turi būti perduodami į taktinių ir strateginių sprendimų lygmenis. Tokiu būdu modelis nėra vienakryptė valdymo schema. Jis grindžiamas nuolatinio mokymosi ir tobulinimo logika, kai operacinė patirtis, incidentų analizė, audito rezultatai, technologinės stebėsenos duomenys ir brandos vertinimas tampa pagrindu koreguoti politikas, procedūras, atsakomybes ir strateginius prioritetus.

Trečiąją modelio dalį sudaro keturi horizontalieji valdymo lygmenys: strateginis, taktinis, operacinis ir technologinis. Šie lygmenys leidžia struktūruoti kibernetinio saugumo valdymą pagal sprendimų priėmimo, koordinavimo, praktinio įgyvendinimo ir techninės realizacijos logiką.

Strateginis lygmuo modelyje atitinka aukščiausią organizacinės ir institucinės krypties formavimo lygį. Jame apibrėžiama kibernetinio saugumo vizija, tikslai, rizikos tolerancija ir atsparumo siekiniai. Šiame lygmenyje kibernetinis saugumas siejamas su e. sveikatos sistemos patikimumu, pacientų pasitikėjimu, paslaugų tęstinumu ir nacionalinės reikšmės informacinės infrastruktūros apsauga. Strateginis lygmuo nustato bendrą saugumo valdymo kryptį ir apibrėžia, kokio saugumo brandos lygio siekiama e. sveikatos sistemoje.

Taktinis, arba valdymo, lygmuo veikia kaip tarpinė grandis tarp strateginių tikslų ir praktinio įgyvendinimo. Šiame lygmenyje strateginės nuostatos transformuojamos į kibernetinio saugumo politikas, procedūras, atsakomybių paskirstymą ir standartus. Taktinis lygmuo yra ypač svarbus todėl, kad būtent čia formuojamos organizacinės taisyklės, lemiančios, kaip kibernetinio saugumo reikalavimai įgyvendinami sveikatos priežiūros įstaigose, nacionalinėse informacinėse sistemose, duomenų mainų procesuose ir sąveikoje su išoriniais paslaugų teikėjais.

Operacinis lygmuo apima kasdienius kibernetinio saugumo valdymo procesus. Šiame lygmenyje įgyvendinamas prieigos valdymas, incidentų registravimas, reagavimo veiksmai ir duomenų apsaugos reikalavimų vykdymas. Operacinis lygmuo parodo faktinį kibernetinio saugumo valdymo veikimą praktikoje, ar strateginės nuostatos ir taktinės procedūros realiai taikomos, ar naudotojų prieigos teisės valdomos tinkamai, ar incidentai registruojami nuosekliai, ar reagavimo veiksmai koordinuojami, o duomenų apsauga užtikrinama ne tik formaliai, bet ir kasdienėje veikloje.

Technologinis lygmuo sudaro techninį modelio pagrindą. Šiame lygmenyje išskiriamos informacinių sistemų apsaugos ir stebėsenos priemonės, o su technologiniu įgyvendinimu taip pat siejami atsarginių kopijų, duomenų apsaugos ir medicininių prietaisų interneto saugumo elementai. Technologinis lygmuo apima prieigos kontrolę, tinklo segmentavimą, grėsmių stebėseną, sistemų atnaujinimą, atsarginių kopijų valdymą, duomenų vientisumo užtikrinimą ir IoMT saugumo priemones (Alharbi ir Alkhalifah, 2025; Clarke ir Martin, 2024). E. sveikatos sistemos kontekste šis lygmuo ypač svarbus dėl didelio informacinių sistemų integracijos masto, jautrių sveikatos duomenų apdorojimo, medicininių prietaisų prijungimo prie tinklų ir paslaugų tęstinumo reikalavimų. Vis dėlto technologinis lygmuo neturi būti suvokiamas kaip savarankiškas ar dominuojantis modelio elementas. Jis užtikrina, kad strateginiai, organizaciniai ir procesiniai sprendimai būtų realizuojami konkrečiomis techninėmis priemonėmis.

Toks valdymo lygmenų atskyrimas leidžia pagrįsti modelį kaip kompleksinę e. sveikatos kibernetinio saugumo valdysenos struktūrą. Sveikatos sistemos pažeidžiamumų analizė rodo, kad vien technologinių priemonių diegimas nėra pakankamas, jeigu nėra aiškių sprendimų priėmimo, atsakomybių paskirstymo, incidentų koordinavimo ir organizacinio mokymosi mechanizmų (Brantly, 2026). Todėl kuriamas modelis orientuojamas ne į atskirų saugumo priemonių sąrašą, bet į valdymo brandos didinimą.

Ketvirtąją modelio dalį sudaro šešios funkcinės kibernetinio saugumo valdymo dimensijos, vertikaliai kertančios visus keturis valdymo lygmenis: rizikų valdymas, incidentų valdymas, technologinis saugumas, duomenų apsauga, atitiktis teisės aktams ir brandos vertinimas. Šios dimensijos nėra izoliuotos sritys. Jos veikia kaip tarp lygmeninės valdymo kryptys, kurios turi būti integruotos į strateginius, taktinius, operacinius ir technologinius sprendimus.

Rizikų valdymo dimensija apima grėsmių, pažeidžiamumų, poveikio ir rizikos tolerancijos vertinimą. Strateginiame lygmenyje ji padeda nustatyti priimtiną rizikos lygį ir prioritetus, taktiniame lygmenyje – formuoti rizikų valdymo procedūras, operaciniame lygmenyje – stebėti ir registruoti rizikos įvykius, o technologiniame lygmenyje – taikyti technines rizikos mažinimo priemones.

Incidentų valdymo dimensija apima incidentų prevenciją, aptikimą, registravimą, klasifikavimą, reagavimą, atkūrimą ir analizę po incidento. E. sveikatos sistemoje ši dimensija tiesiogiai susijusi su paslaugų tęstinumu ir pacientų sauga, nes informacinių sistemų neprieinamumas ar duomenų vientisumo pažeidimas gali turėti praktinių pasekmių sveikatos priežiūros paslaugų teikimui.

Technologinio saugumo dimensija apima informacinių sistemų, tinklų,

infrastruktūros, medicininių prietaisų, stebėsenos sprendimų ir techninių apsaugos priemonių valdymą. Ji užtikrina, kad kibernetinio saugumo valdymo sprendimai būtų paremti tinkamomis technologinėmis kontrolės priemonėmis, kurios turi būti nuolat stebimos, atnaujinamos ir vertinamos.

Duomenų apsaugos dimensija yra viena esminių e. sveikatos sistemos saugumo sričių, nes sistemoje tvarkomi jautrūs asmens sveikatos duomenys. Ji apima duomenų konfidencialumo, vientisumo, prieinamumo, atsekamumo, teisėto naudojimo, prieigos kontrolės ir duomenų gyvavimo ciklo valdymo aspektus. Modelyje duomenų apsauga siejama ne tik su techniniu duomenų šifravimu ar prieigos ribojimu, bet ir su organizacinėmis taisyklėmis, naudotojų atsakomybėmis ir procesų kontrole.

Atitikties teisės aktams dimensija apima kibernetinio saugumo, asmens duomenų apsaugos, sveikatos duomenų tvarkymo ir informacinių sistemų saugos reikalavimų įgyvendinimą. Ji užtikrina, kad e. sveikatos sistemos kibernetinio saugumo valdymas būtų suderintas su nacionaliniais teisės aktais, Europos Sąjungos reguliavimu, standartais ir institucine atsakomybe. Ši dimensija svarbi todėl, kad e. sveikatos sistema veikia griežtai reguliuojamoje aplinkoje, kurioje saugumo valdymas turi būti pagrįstas ne tik organizaciniais sprendimais, bet ir teisiniais įsipareigojimais.

Brandos vertinimo dimensija atlieka nuolatinio tobulinimo funkciją. Ji leidžia vertinti, kiek kibernetinio saugumo valdymo procesai yra formalizuoti, integruoti, taikomi praktikoje, matuojami ir tobulinami. Brandos vertinimas padeda pereiti nuo formalaus reikalavimų įgyvendinimo prie sistemingo saugumo valdymo, leidžiančio identifikuoti spragas, prioritetus ir tobulinimo kryptis.

Penktoji modelio dalis yra kibernetinio saugumo valdymo branduolys. Jis simbolizuoja holistinį ir integruotą požiūrį į kibernetinį saugumą e. sveikatos sistemoje ir jungia valdymo lygmenis, funkcines dimensijas, grįžtamąjį ryšį ir e. sveikatos sistemos kontekstą į vieną sistemą. Branduolys parodo, kad kibernetinio saugumo valdymas nėra strategijos, procedūrų ar technologijų suma. Tai koordinavimo mechanizmas, kuriame turi būti suderinti strateginiai tikslai, atsakomybės, operaciniai procesai, techninės priemonės, duomenų apsauga, atitiktis teisės aktams, brandos vertinimas ir e. sveikatos sistemos veikimo poreikiai.

Modelio centre pavaizduotos sąveikos rodyklės ir tarp dimensiniai mazgai žymi, kad kiekvienas valdymo lygmuo ir kiekviena funkcinė dimensija turi sąsajų su kitomis modelio dalimis. Pavyzdžiui, incidentų valdymas negali būti veiksmingas be rizikų vertinimo, technologinės stebėsenos, aiškių procedūrų, duomenų apsaugos reikalavimų ir atsakomybių paskirstymo. Taip pat brandos vertinimas negali būti atsietas nuo operacinės praktikos, nes būtent kasdieniai incidentai, audito rezultatai, prieigos valdymo trūkumai ir paslaugų sutrikimai parodo realų organizacijos saugumo lygį.

Šeštoji modelio dalis yra e. sveikatos sistemos kontekstas, modelyje išskirtas kaip apatinė konceptuali platforma. Joje įvardijami pagrindiniai e. sveikatos sistemos elementai: pacientų sauga, klinikiniai procesai, sveikatos duomenys, sistemų sąveika, medicininiai prietaisai ir paslaugų tęstinumas. Šis kontekstas pabrėžia, kad modelis nėra bendro pobūdžio kibernetinio saugumo schema. Jis orientuotas į e. sveikatos sistemos tobulinimą, todėl kibernetinio saugumo valdymas turi būti siejamas su klinikinių

procesų patikimumu, pacientų duomenų apsauga, sistemų integracija, medicininių technologijų saugumu ir sveikatos paslaugų nepertraukiamumu.

Modelyje naudojamos rodyklės ir sąveikos linijos atlieka analitinę, o ne dekoratyvinę funkciją. Tiesioginės rodyklės žymi valdymo kryptį iš strateginio į technologinį lygmenį. Punktyrinės rodyklės žymi grįžtamąjį ryšį iš technologinio ir operacinio lygmenų į taktinius bei strateginius sprendimus. Dvikryptės rodyklės parodo sąveiką tarp valdymo lygių, funkcinių dimensijų ir e. sveikatos sistemos konteksto elementų. Sąveikos taškai žymi tarp dimensinius mazgus, kuriuose susikerta skirtingi valdymo aspektai. Tokia vizualinė logika leidžia parodyti, kad e. sveikatos kibernetinio saugumo valdymas yra ne linijinis, bet kompleksinis, ciklinis ir nuolat tobulinamas procesas.

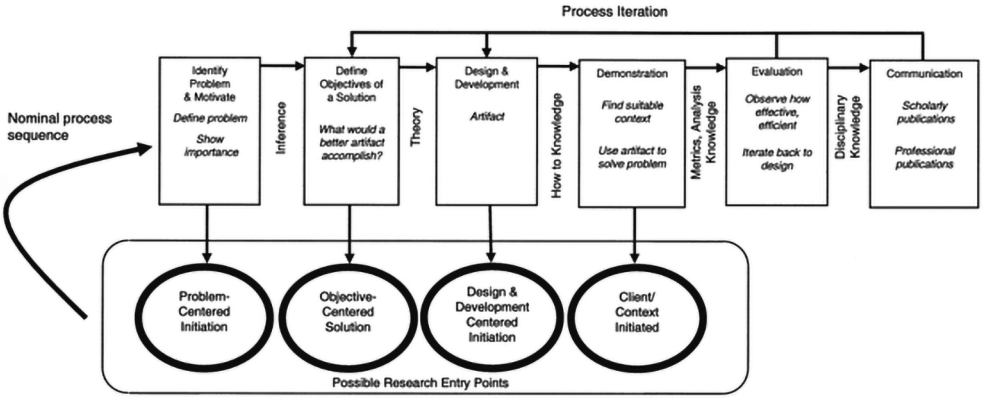
Apibendrinant galima teigti, kad pradiniame teoriniame modelyje kibernetinio saugumo valdymas suprantamas kaip integruota daugialypė sistema, kurioje strateginiai sprendimai, taktiniai valdymo mechanizmai, operaciniai procesai, technologinės priemonės, funkcinės saugumo dimensijos ir e. sveikatos sistema veikia tarpusavyje. Modelis leidžia sistemiškai struktūruoti kibernetinio saugumo valdymo lauką e. sveikatos sistemoje ir sudaro pagrindą tolesniam empiriniam vertinimui.

Svarbu pabrėžti, kad šiame poskyryje pateikiamas modelis yra pradinis teorinis kibernetinio saugumo valdymo modelis, suformuotas remiantis mokslinės literatūros, tarptautinių standartų ir konceptualių valdymo modelių analize. Jis skirtas sistemiškai struktūruoti kibernetinio saugumo valdymo lauką e. sveikatos sistemoje, tačiau dar neįtraukia empirinio tyrimo metu identifikuotų praktinių spragų, organizacinių sąsajų ir veiklos nuostatų. Šis pradinis modelis sudaro analitinį atskaitos tašką, kuris vėlesniuose disertacijos skyriuose vertinamas, tikslinamas ir struktūriškai bei funkciškai papildomas remiantis ekspertinio tyrimo rezultatais.

2.4. Tyrimo metodologija

Disertacijos tyrimo metodologija parengta atsižvelgiant į nagrinėjamo objekto – kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui – kompleksiškumą ir daugiamatiškumą. E. sveikatos sistemos apima ne tik techninius informacinių sistemų komponentus, bet ir organizacinius procesus, teisinį reguliavimą, tarp organizacinę sąveiką bei tiesioginę sąsają su pacientų sauga. Dėl šios priežasties tyrimas negali būti grindžiamas vien pavienių rodiklių matavimu ar techninių sprendimų analize, bet reikalauja integruoto, sisteminio ir empiriškai pagrįsto metodologinio požiūrio (Hevner ir kt., 2004).

Atsižvelgiant į tyrimo tikslą – įvertinti ir patikslinti kibernetinio saugumo valdymo modelį e. sveikatos sistemos tobulinimui – disertacijoje taikoma dizaino mokslo tyrimų metodologija (angl. *Design Science Research*). Ši metodologinė paradigma leidžia kryptingai kurti ir tobulinti praktinį artefaktą – kibernetinio saugumo valdymo modelį, remiantis tiek teorinėmis įžvalgomis, tiek empiriniais duomenimis, gautais realiame organizaciniame kontekste (Hevner ir kt., 2004; Peffers ir kt., 2007).



6 pav. Dizaino mokslo tyrimų metodologija

Šaltinis: Peffers, K., Tuunanen, T., Rothenberger, M. A., ir Chatterjee, S. (2007/2008)

Dizaino mokslo tyrimų metodologija orientuota į problemų sprendimą, kuriant ir vertinant artefaktus, tokius kaip modeliai, metodikos ar valdymo sistemos. Ji ypač tinkama kibernetinio saugumo valdymo tyrimams, kuriuose svarbu ne tik konceptualus pagrįstumas, bet ir praktinis taikymas sudėtingose, rizikingose srityse, tokiose kaip e. sveikatos sistema (Aven, 2016). Todėl ši disertacija grindžiama nuoseklia tyrimo struktūra, apimančia teorinę analizę, empirinį ekspertinį vertinimą ir modelio tikslinimą.

Pirmuoju tyrimo etapu atliekama išsami mokslinės literatūros analizė, apimanti kibernetinio saugumo valdymo teorinius modelius, tarptautinius standartus, reguliacinius reikalavimus ir brandos vertinimo metodikas. Šis etapas leidžia identifikuoti pagrindines kibernetinio saugumo valdymo dimensijas, jų tarpusavio sąsajas bei problemas, kurios yra ypač aktualios e. sveikatos sistemoms (Ransbotham ir kt., 2012, Sandelowski, 2010).

Antruoju etapu kuriamas konceptualus kibernetinio saugumo valdymo modelis, orientuotas į e. sveikatos sistemos tobulinimą. Modelio struktūra grindžiama hierarchiniu valdymo lygių išdėstymu ir funkcinėmis saugumo valdymo dimensijomis, apimančiomis strateginį, organizacinį, procesinį ir technologinį lygmenis. Šios dimensijos vėliau tampa empirinio vertinimo pagrindu. Tokia metodologinė seka atitinka dizaino mokslo tyrimų rekomendacijas, kuriose pabrėžiamas nuoseklus perėjimas nuo problemos identifikavimo prie sprendimo konstravimo ir jo vertinimo realiame kontekste (Peffers ir kt., 2007).

Trečiuoju etapu atliekamas empirinis tyrimas, taikant kokybinį tyrimo metodą – pusiau struktūrizuotus ekspertinius interviu. Ekspertinis interviu pasirinktas kaip pagrindinis empirinių duomenų rinkimo metodas, nes kibernetinio saugumo valdymas e. sveikatos sistemoje yra sudėtingas, kontekstinis ir aukštos specializacijos reikalaujantis reiškinys, kurio negalima adekvačiai atskleisti vien standartizuotais klausimynais ar kiekybiniais rodikliais (Žydžiūnaitė, Sabaliauskas, 2017; Kardelis, 2019).

Ekspertiniai interviu leidžia atskleisti realias kibernetinio saugumo valdymo praktikas, sprendimų priėmimo logiką, organizacinius apribojimus bei kontekstinius veiksnius, darančius įtaką saugumo brandai e. sveikatos sistemoje. Šis metodas suteikia galimybę integruoti strateginę, organizacinę ir technologinę perspektyvas bei identifikuoti ne tik esamą valdymo lygį, bet ir sistemines spragas bei tobulinimo kryptis (Venkatesh ir kt., 2013).

Svarbi tyrimo metodologijos dalis yra kibernetinio saugumo brandos vertinimo logikos integravimas kaip analitiniu vertinimo pagrindu. Brandos požiūris leidžia analizuoti kibernetinio saugumo valdymą ne kaip pavienių priemonių rinkinį, bet kaip nuosekliai besivystančią valdymo sistemą, apimančią procesų formalizavimą, atsakomybių paskirstymą, kontrolės mechanizmus ir nuolatinio tobulinimo praktikas (Singer ir Friedman, 2014).

Disertacijoje brandos vertinimo logika taikoma analizuojant ekspertų pateiktas įžvalgas ir vertinimus, leidžiančius identifikuoti esamą kibernetinio saugumo valdymo lygį e. sveikatos institucijose bei nustatyti prioritetines tobulinimo sritis. Brandos kategorijos ir rodikliai naudojami kaip konceptualus analitinis karkasas, kuris vėliau detalizuojamas empirinių rezultatų analizėje 3 skyriuje.

Apibendrinant galima teigti, kad pasirinkta tyrimo metodologija yra nuosekliai suderinta su disertacijos tema ir tikslais. Dizaino mokslo tyrimų metodologija sudaro pagrindą kibernetinio saugumo valdymo modelio kūrimui, ekspertinis interviu leidžia empiriškai įvertinti jo taikymo praktiką, o brandos vertinimo logika suteikia galimybę identifikuoti sistemines spragas ir tobulinimo kryptis e. sveikatos sistemoje (Hevner ir kt., 2004; Peffers ir kt., 2007).

Tokiu būdu tyrimo metodologija užtikrina teorinį pagrįstumą, empirinį patikimumą ir praktinį aktualumą, sudarydama sąlygas išsamiai analizuoti ekspertinio tyrimo rezultatus ir tobulinti siūlomą kibernetinio saugumo valdymo modelį.

2.4.1. Tyrimo tikslas, uždaviniai ir tiriamieji klausimai

Šio disertacinio tyrimo metodologinis pagrindas formuojamas atsižvelgiant į ankstesniuose skyriuose išanalizuotą kibernetinio saugumo valdymo teoriją, informacijos saugumo valdymo sistemas, brandos modelius ir e. sveikatos sektoriaus specifiką. Atlikta teorinė analizė atskleidė, kad egzistuojantys kibernetinio saugumo valdymo modeliai dažnai nėra pakankamai pritaikyti kompleksiškoms, tarp organizacinėms ir aukštos rizikos e. sveikatos sistemoms. Dėl šios priežasties išlieka poreikis struktūruotam, empiriškai pagrįstam kibernetinio saugumo valdymo modeliui, orientuotam ne tik į apsaugą, bet ir į sisteminį e. sveikatos sistemos tobulinimą.

Šio disertacinio **tyrimo tikslas** – sukurti ir empiriškai įvertinti kibernetinio saugumo valdymo modelį, skirtą e. sveikatos sistemos tobulinimui, integruojant strateginius, organizacinius, procesinius, technologinius ir reguliacinius aspektus bei įvertinant jo taikymo efektyvumą praktiniame kontekste.

Šis tikslas atitinka dizaino mokslo tyrimų metodologijos (angl. *Design Science Research*) logiką, kurioje akcentuojamas ne tik teorinis reiškinio pažinimas, bet ir

praktiškai pritaikomo valdymo modelio sukūrimas, empirinė jo analizė ir tobulinimas realioje organizacinėje aplinkoje.

Siekiant įgyvendinti iškeltą tyrimo tikslą, disertacijoje formuluojami šie **tyrimo uždaviniai:**

1. Išanalizuoti kibernetinio saugumo valdymo teorinius pagrindus, apimančius informacijos saugumo valdymo sistemas, brandos modelius, rizikų ir incidentų valdymo koncepcijas bei jų taikymą e. sveikatos sistemų kontekste.
2. Ištirti e. sveikatos sistemoms būdingas kibernetines grėsmes, rizikos veiksnius ir incidentų pasekmes, siekiant identifikuoti kritines valdymo spragas ir sisteminius pažeidžiamumus.
3. Išanalizuoti esamus teorinius ir praktinius kibernetinio saugumo valdymo modelius, įvertinant jų tinkamumą e. sveikatos sistemų valdymui ir tobulinimui.
4. Sukurti integruotą kibernetinio saugumo valdymo modelį, pritaikytą e. sveikatos sistemoms, apimantį valdymo lygius, funkcines dimensijas, informacijos srautus ir atsakomybių paskirstymą.
5. Parengti empirinio tyrimo instrumentus, leidžiančius struktūruotai rinkti ekspertines įžvalgas apie kibernetinio saugumo valdymo praktiką, brandos lygį ir tobulinimo poreikius e. sveikatos sistemoje.
6. Atlikti empirinį tyrimą, taikant pusiau struktūrizuotus ekspertinius interviu, siekiant įvertinti kibernetinio saugumo valdymo būklę e. sveikatos sistemoje ir analizuoti sukurto modelio taikymo praktinį tinkamumą.
7. Remiantis ekspertinio tyrimo rezultatais, patikslinti kibernetinio saugumo valdymo modelį ir suformuluoti rekomendacijas jo taikymui e. sveikatos sistemos tobulinimo procesuose.

Atsižvelgiant į tyrimo tikslą, uždavinius ir pasirinktą kokybinę dizaino mokslo tyrimų metodologiją, disertacijoje formuluojami šie tiriamieji klausimai (TK1–TK4), į kuriuos atsakoma remiantis ekspertinių interviu duomenų temine analize ir ekspertų vertinimų interpretacija teorinės bei dokumentų analizės kontekste (žr. 2–5 priedus):

TK1. Kaip ekspertai vertina kibernetinio saugumo valdymo organizavimą e. sveikatos organizacijose ir kokie jo fragmentiškumo požymiai išryškėja ekspertų vertinimuose?

TK2. Kaip ekspertai vertina strateginio, taktinio, operacinio ir technologinio kibernetinio saugumo valdymo lygmenų integraciją e. sveikatos organizacijose ir kokie šios integracijos ribotumai išryškėja praktikoje?

TK3. Kaip ekspertai sieja kibernetinio saugumo valdymo struktūrizuotumą su kibernetinių incidentų valdymo veiksmingumu e. sveikatos organizacijose?

TK4. Kaip ekspertai vertina siūlomo kibernetinio saugumo valdymo modelio galimą indėlį stiprinant organizacinį pasirengimą kibernetinėms grėsmėms e. sveikatos sistemos kontekste?

2.4.2. Tyrimo dizainas

Atsižvelgiant į disertacijos tikslą, uždavinius ir suformuluotus tiriamuosius klausimus, pasirinktas kokybinis tyrimo dizainas, grindžiamas dizaino mokslo tyrimų metodologija (angl. Design Science Research). Toks tyrimo dizainas leidžia nuosekliai derinti teorinę analizę, konceptualaus modelio kūrimą ir ekspertinį empirinį vertinimą, užtikrinant gilų ir kontekstualų nagrinėjamo reiškinio pažinimą.

Sekvencinio kokybinio tyrimo dizaino esmė – nuoseklūs, tarpusavyje susiję tyrimo etapai, kai ankstesnio etapo rezultatai tampa pagrindu vėlesniems sprendimams ir analizėms. Šiame disertaciniame tyrime taikoma validacinė seka, kuri leidžia pirmiausia identifikuoti ir struktūruoti kibernetinio saugumo valdymo problematiką, vėliau sukurti teorinį modelį ir galiausiai empiriškai įvertinti jo tinkamumą e. sveikatos sistemos kontekste, remiantis ekspertų patirtimi ir įžvalgomis.

Pirmajame tyrimo etape atliekama išsami mokslinės literatūros, tarptautinių standartų, brandos modelių, reguliacinių dokumentų ir gerosios praktikos analizė. Šio etapo tikslas – identifikuoti esmines kibernetinio saugumo valdymo dimensijas, jų tarpusavio sąsajas, valdymo lygius ir problemas, būdingas e. sveikatos sistemoms. Teorinė analizė sudaro konceptualų pagrindą tolesniam modelio konstravimui ir leidžia užtikrinti teorinį tyrimo nuoseklumą.

Antrajame etape kuriamas konceptualus kibernetinio saugumo valdymo modelis, orientuotas į e. sveikatos sistemos tobulinimą. Modelio struktūra formuojama remiantis hierarchiniu valdymo lygių išdėstymu, funkcinėmis saugumo valdymo dimensijomis, informacijos srautais, atsakomybių paskirstymu ir kibernetinio atsparumo operacionalizavimo logika. Šis etapas atitinka dizaino mokslo tyrimų logiką, kurioje akcentuojamas artefakto kūrimas kaip atsakas į identifikuotą praktinę problemą (Hevner ir kt., 2004; Peffers ir kt., 2007).

Trečiajame tyrimo etape vykdomas empirinis kokybinis tyrimas, taikant pusiau struktūrizuotus ekspertinius interviu. Ekspertai, turintys ilgametę patirtį kibernetinio saugumo, e. sveikatos sistemų, viešojo sektoriaus ar reguliacinio valdymo srityse, vertina esamą kibernetinio saugumo valdymo praktiką, identifikuoja spragas, pateikia įžvalgas apie modelio taikymo galimybes ir tobulinimo kryptis. Šis etapas leidžia įvertinti modelio praktinį tinkamumą, kontekstinį aktualumą ir pritaikomumą e. sveikatos sistemoje.

Gauti ekspertinio tyrimo rezultatai naudojami ketvirtajame etape – modelio tikslinimo ir validavimo procese, kuriame integruojamos ekspertų įžvalgos, identifikuotos problemos ir siūlomi sprendimai. Tokiu būdu tyrimas įgyja ciklinį pobūdį, būdingą dizaino mokslo tyrimams, kai modelis ne tik kuriamas, bet ir tobulinamas remiantis empiriniais duomenimis.

Svarbu pažymėti, kad šiame tyrime kibernetinio saugumo valdymo modelio poveikis e. sveikatos sistemos atsparumui nėra tikrinamas eksperimentiniu ar priežastinio poveikio vertinimo būdu. Tyrime nėra lyginami faktiniai atsparumo rodikliai prieš modelio taikymą ir po jo taikymo, pavyzdžiui, incidentų aptikimo laikas, reagavimo laikas, paslaugų atkūrimo trukmė ar kritinių e. sveikatos paslaugų prieinamumo

pokytis. Todėl disertacijoje modelio reikšmė formuluojama kaip teorinėmis prielaidomis, ekspertiniu vertinimu ir operaciniais atsparumo rodikliais pagrįstų prielaidų e. sveikatos sistemos kibernetiniam atsparumui didinti sukūrimas.

Tokia metodologinė pozicija leidžia aiškiai atskirti modelio konceptualų ir praktinį pagrįstumą nuo faktinio priežastinio poveikio matavimo. Ekspertinis tyrimas šiame darbe naudojamas modelio struktūros, aktualumo, taikymo galimybių ir atsparumo didinimo prielaidų vertinimui, tačiau pats atsparumo pokytis galėtų būti tikrinamas tik vėlesniuose tyrimuose, taikant pasirengimo, aptikimo, reagavimo, atkūrimo, paslaugų tęstinumo, mokymosi ir organizacinės brandos rodiklius.

Pasirinktas tyrimo dizainas atitinka tyrimų metodologijos principus, kuriuose pabrėžiama, kad sudėtingų sistemų, tokių kaip e. sveikatos infrastruktūra, tyrimai turi būti grindžiami ne vien teorinėmis prielaidomis, bet ir giliu kontekstiniu supratimu, gaunamu iš praktikoje veikiančių ekspertų (Hevner ir kt., 2004; Peffers ir kt., 2007). Ekspertinio tyrimo taikymas leidžia sumažinti formalų abstraktumą ir sustiprinti disertacijos praktinį aktualumą.

Šiame disertaciniame tyrime sukurtas kibernetinio saugumo valdymo modelis traktuojamas kaip konceptualus vadybinis artefaktas, kurio paskirtis – sistemiškai struktūruoti kibernetinio saugumo valdymo elementus e. sveikatos sistemos tobulinimo kontekste. Toks tyrimo dizainas atitinka dizaino mokslo tyrimų logiką, pagal kurią tyrėjas kuria ir vertina artefaktą – modelį, metodą, konstrukciją ar valdymo sprendimą, skirtą aktualiai organizacinei ar technologinei problemai spręsti (Hevner ir kt., 2004; Peffers ir kt., 2007). Dizaino mokslo požiūriu modelio vertinimas gali būti atliekamas ne tik tiesiogiai matuojant jo taikymo poveikį organizacijoje, bet ir vertinant jo vidinį nuoseklumą, atitikimą probleminei sričiai, pritaikomumą ir praktinį pagrįstumą ekspertų vertinimo būdu.

Atsižvelgiant į tai, šiame darbe ekspertinis vertinimas taikomas ne kaip faktinio modelio efektyvumo įrodymas, o kaip konceptualaus ir praktinio modelio tinkamumo patikrinimas. Ekspertų įžvalgos leidžia įvertinti, ar modelio struktūrinės dalys, valdymo lygmenys, atsakomybių pasiskirstymas, rizikų ir incidentų valdymo elementai atitinka realias e. sveikatos sistemos kibernetinio saugumo valdymo sąlygas.

Apibendrinant galima teigti, kad pasirinktas kokybinis tyrimo dizainas yra tinkamas disertacijos tikslui, nes sudaro prielaidas sistemiškai analizuoti kibernetinio saugumo valdymą e. sveikatos sistemoje, sukurti moksliškai pagrįstą modelį ir empiriškai įvertinti jo taikymo galimybes realiame organizaciniame kontekste. Kartu šis tyrimo dizainas leidžia pagrįsti modelio sudaromas prielaidas e. sveikatos sistemos kibernetiniam atsparumui didinti. Toks metodologinis apibrėžimas užtikrina tyrimo nuoseklumą, empirinį pagrįstumą ir aiškiai apibrėžia disertacijos rezultatų interpretavimo ribas.

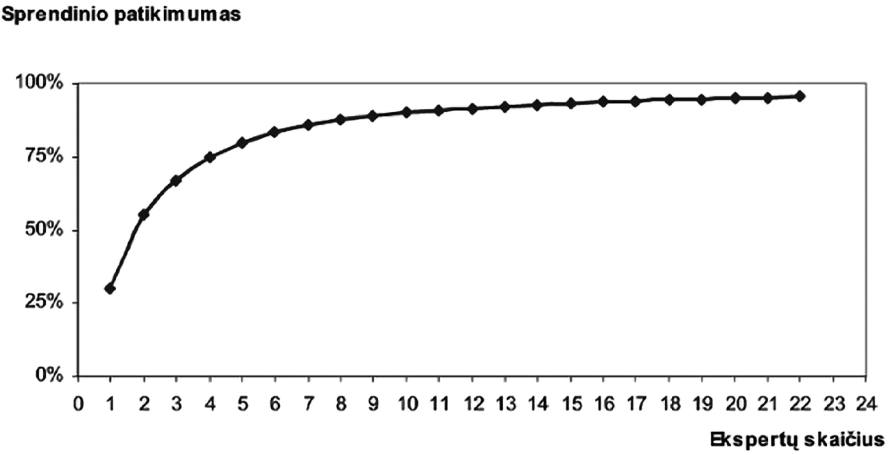
2.4.3. Tyrimo imtis, ekspertų atranka ir atrankos kriterijai

Šiame disertaciniame tyrime taikyta tikslinė (ekspertinė) imties atranka, kuri yra būdinga kokybiniams tyrimams, kai siekiama giliai, sistemiškai įvertinti sudėtingus,

aukštos specializacijos reikalaujančius reiškinius, tokius kaip kibernetinio saugumo valdymas e. sveikatos sistemoje (Žydžiūnaitė, Sabaliauskas, 2017; Kardelis, 2019). Atsižvelgiant į tyrimo tikslą – empiriškai įvertinti ir patikslinti kibernetinio saugumo valdymo modelį e. sveikatos sistemos tobulinimui – respondentais pasirinkti kibernetinio saugumo srities ekspertai, turintys ilgametę profesinę, institucinę ir (ar) strateginę patirtį (13 lentelė).

Ekspertinio tyrimo imties dydis buvo nustatomas remiantis ekspertinių vertinimų patikimumo teorinėmis prielaidomis, kuriose teigiama, kad agreguotų ekspertinių sprendimų patikimumas ir ekspertų skaičius siejami netiesiniu, greitai gęstančiu ryšiu (Augustinaitis ir kt., 2009). Tai reiškia, kad didėjant ekspertų skaičiui sprendimų patikimumas auga tik iki tam tikros ribos, o vėliau papildomas ekspertų skaičiaus didinimas nebesukuria proporcingos analitinės ar metodologinės pridėtinės vertės.

Ši metodologinė nuostata iliustruojama sprendimo patikimumo ir ekspertų skaičiaus priklausomybės grafiku (žr. 7 pav.), kuriame matyti, kad jau esant 7 – 9 ekspertams pasiekiamas aukštas vertinimų stabilumo ir patikimumo lygis.



7 pav. Ekspertų skaičiaus įtaka vertinimo patikimumui

Šaltinis: Augustinaitis ir kt. (2009)

Vadovaujantis šiomis metodologinėmis prielaidomis, taip pat atsižvelgiant į tyrimo objekto – kibernetinio saugumo valdymo e. sveikatos sistemoje – kompleksiškumą ir tarpdisciplininį pobūdį, šiame disertaciniame tyrime buvo pasirinkta devynių ekspertų imtis. Toks ekspertų skaičius laikomas metodologiškai pagrįstu ir pakankamu gauti patikimus ir analitiškai reikšmingus kokybinius duomenis (Augustinaitis ir kt., 2009).

Pažymėtina, kad kokybiniuose tyrimuose imties pakankamumas vertinamas ne tik kiekybiškai, bet ir vadovaujantis duomenų prisotinimo principu, momentu, kai naujai gaunami duomenys nebesukuria iš esmės naujų temų, kategorijų ar interpretacinių

įžvalgų (Guest, Bunce ir Johnson, 2006; Kardelis, 2019). Tyrimo metu nustatyta, kad devynių ekspertų pateiktos įžvalgos leido pasiekti teminį ir analitinį prisotinimą, o papildomi interviu nebesuteiktų reikšmingai naujos informacijos.

Šiame disertaciniame tyrime taikyta tikslinė ekspertinė atranka, grindžiama ne atsitiktiniu respondentų parinkimu, o informacinės vertės, profesinės kompetencijos ir tyrimo problemos išmanymo kriterijais. Tikslinė atranka laikoma tinkama kokybiniuose tyrimuose, kai siekiama gauti ne statistiškai reprezentatyvią, o analitiškai reikšmingą informaciją iš asmenų, turinčių tiesioginės patirties tiriamo reiškinio srityje (Palinkas ir kt., 2015; Malterud ir kt., 2016; Braun ir Clarke, 2006). Kadangi disertacijos objektas yra kibernetinio saugumo valdymo modelio vertinimas e. sveikatos sistemos kontekste, ekspertai buvo atrenkami pagal iš anksto apibrėžtus įtraukimo, atmetimo ir šališkumo mažinimo kriterijus.

Ekspertų įtraukimo į tyrimą kriterijai buvo šie:

1. ne mažesnė kaip penkerių metų profesinė patirtis bent vienoje iš šių sričių: kibernetinio saugumo valdymas, informacijos saugos vadyba, e. sveikatos sistemų administravimas, sveikatos sektoriaus informacinių sistemų kūrimas, diegimas ar priežiūra, viešojo sektoriaus skaitmenizacijos arba kritinės informacinės infrastruktūros valdymas;
2. tiesioginė praktinė arba strateginė sąsaja su sveikatos sektoriaus informacinėmis sistemomis, e. sveikatos infrastruktūra, kibernetinio saugumo politika, rizikų valdymu, incidentų valdymu arba duomenų apsaugos procesais;
3. gebėjimas vertinti ne tik techninius, bet ir organizacinius, vadybinius, procesinius bei reguliacinius kibernetinio saugumo valdymo aspektus;
4. užimamos arba anksčiau eitos pareigos, susijusios su sprendimų priėmimu, konsultavimu, auditu, priežiūra, strateginiu planavimu ar informacinių sistemų saugumo užtikrinimu;
5. pasirengimas dalyvauti pusiau struktūruotame ekspertiniame interviu ir pateikti argumentuotą vertinimą dėl siūlomo modelio struktūros, pritaikomumo, ribotumų ir tobulinimo krypčių.

Siekiant sumažinti atrankos šališkumo riziką, taip pat buvo taikyti ekspertų atmetimo kriterijai. Į tyrimą nebuvo įtraukiami asmenys, kurie: neturėjo tiesioginės profesinės sąsajos su kibernetinio saugumo, informacijos saugos, e. sveikatos arba sveikatos sektoriaus informacinių sistemų valdymo sritimis, galėjo vertinti modelį tik iš siauro techninio arba tik administracinio požiūrio, neturėdami platesnio sisteminio supratimo apie e. sveikatos infrastruktūrą, turėjo tiesioginį interesų konfliktą, galintį lemti neobjektyvų modelio vertinimą.

Atrenkant ekspertus buvo siekiama ne vienodos, o įvairialypės ekspertinės patirties. Todėl imtis formuota vadovaujantis maksimalios variacijos principu: į tyrimą įtraukti skirtinguose įstaigose dirbantys ekspertai, kurių patirtis apėmė viešojo sektoriaus informacinių sistemų valdymą, sveikatos sektoriaus skaitmenizaciją, kibernetinio saugumo politiką, organizacinį saugumo valdymą, technines saugumo priemones, rizikų ir incidentų valdymą. Toks atrankos principas leido išvengti vienos profesinės grupės dominavimo ir sudarė sąlygas modelį vertinti iš kelių tarpusavyje susijusių

perspektyvų: strateginės, organizacinės, technologinės, procesinės ir reguliacinės.

Ekspertų atrankos griežtumas buvo užtikrinamas keliais etapais. Pirma, buvo identifikuotos tyrimui aktualios kompetencijų sritys, atitinkančios modelio struktūrinius komponentus. Antra, potencialūs ekspertai buvo vertinami pagal profesinės patirties, institucinės patirties, sąsajos su e. sveikatos arba kritinės informacinės infrastruktūros valdymu ir gebėjimo vertinti modelį sistemiškai kriterijus. Trečia, prieš įtraukiant ekspertą į tyrimą buvo įvertinama galima interesų konflikto, institucinės priklausomybės arba pernelyg siauro profesinio požiūrio rizika. Ketvirta, interviu metu gauti duomenys buvo analizuojami ne kaip pavienės nuomonės, o kaip argumentuotų ekspertinių vertinimų visuma, ieškant pasikartojančių temų, sutapimų, prieštaravimų ir modelio tikslinimui reikšmingų įžvalgų.

Tyrimo imties dydis buvo grindžiamas informacinės galios principu. Kokybiniuose tyrimuose imties pakankamumas priklauso ne tik nuo respondentų skaičiaus, bet ir nuo tyrimo tikslo aiškumo, ekspertų patirties specifiškumo, interviu gilumo ir gautų duomenų aktualumo tyrimo klausimams (Malterud, Siersma ir Guassora, 2016).

Siekiant mažinti subjektyvumo poveikį, tyrime taikytos kelios metodologinės kontrolės priemonės. Pirma, visiems ekspertams buvo pateikiamas tas pats pusiau struktūruoto interviu klausimynas, leidęs užtikrinti teminį interviu palyginamumą. Antra, ekspertų atsakymai buvo analizuojami taikant teminę analizę, leidžiančią sistemiškai identifikuoti pasikartojančias temas, argumentų kryptis ir problemines sritis (Braun ir Clarke, 2006). Trečia, ekspertų įžvalgos buvo lyginamos su teorinės analizės, teisės aktų, tarptautinių standartų ir dokumentų analizės rezultatais, taip taikant duomenų trianguliacijos principą. Ketvirta, tyrimo rezultatų interpretavime buvo atskiriamos individualios ekspertų nuomonės nuo pasikartojančių, kelių ekspertų patvirtintų teminių įžvalgų. Penkta, ekspertams suteiktas anonimiškumas sumažino socialiai pageidaujamų atsakymų, institucinio atsargumo ir hierarchinio spaudimo riziką.

Toks ekspertų atrankos ir duomenų analizės organizavimas leidžia pagrįsti, kad ekspertinis vertinimas šiame tyrime nėra atsitiktinė ar subjektyviai parinkta nuomonių visuma. Priešingai, ekspertų atranka buvo grindžiama aiškiais profesinės kompetencijos, praktinės sąsajos, tarpdisciplininio vertinimo gebėjimo ir šališkumo mažinimo kriterijais. Todėl ekspertų vertinimai laikytini tinkamais modelio konceptualiam pagrįstumui, praktiniam aktualumui, taikymo galimybėms ir ribotumams įvertinti, nors jie negali būti interpretuojami kaip statistinis visos sveikatos sektoriaus organizacijų populiacijos atspindys ar faktinio modelio efektyvumo matavimas.

Dauguma apklaustų ekspertų, dirbančių Lietuvoje ir atstovaujančių valstybiniam sektoriui, buvusių valstybės tarnautojų, statutinių pareigūnų bei akademinės bendruomenės narių, yra aktyviai prisidėję prie kibernetinio saugumo sistemos kūrimo Lietuvoje, valstybės kibernetinio saugumo politikos ir strategijos formavimo.

Vadovaujantis tyrimų etikos principais ir asmens duomenų apsaugos reikalavimais (Kardelis, 2019; Žydžiūnaitė, Sabaliauskas, 2017), ekspertams buvo suteikti identifikatoriai (E1–E9), kurie naudojami duomenų analizėje ir rezultatų pateikime, neatskleidžiant nei jų tapatybės, nei konkrečių darboviečių ar pareigų. Ekspertinių interviu informacija pateikiama 13 lentelėje.

13 lentelė. Ekspertų ir interviu informacija

Eksperto identifikatorius	Interviu trukmė (min.)	Interviu data
E1	103 min.	2024-07-08
E2	94 min.	2024-07-09
E3	114 min.	2024-07-11
E4	105 min.	2024-07-15
E5	98 min.	2024-07-16
E6	116 min.	2024-07-18
E7	123 min.	2024-07-22
E8	86 min.	2024-07-23
E9	95 min.	2024-07-25

Šaltinis: sudaryta autorės

Apibendrinant galima teigti, kad pasirinkta tyrimo imtis ir ekspertų atrankos metodas yra metodologiškai pagrįsti, atitinka disertacinio tyrimo tikslus bei užtikrina gautų rezultatų patikimumą, validumą ir analitinį gilumą, reikalingą kibernetinio saugumo valdymo modelio vertinimui ir tobulinimui e. sveikatos sistemos kontekste.

2.4.4. Duomenų rinkimo priemonės

Atsižvelgiant į disertacijos tikslą, duomenų rinkimo priemonės parinktos taip, kad leistų išsamiai atskleisti ekspertinį požiūrį, sprendimų priėmimo logiką bei realias kibernetinio saugumo valdymo problemas. Tyrime taikomos kokybinės duomenų rinkimo priemonės, atitinkančios pasirinkto tyrimo dizaino metodologijos nuostatas.

Pagrindine empirinio tyrimo duomenų rinkimo priemone pasirinktas pusiau struktūrizuotas ekspertinis interviu. Ši priemonė leidžia derinti iš anksto apibrėžtą klausimų struktūrą su lankstumu, suteikiančiu galimybę adaptuoti interviu eigą prie konkrečios eksperto patirties, kompetencijų ir nagrinėjamos problematikos gilumo (Kvale ir Brinkmann, 2015). Pusiau struktūrizuotas interviu yra ypač tinkamas tiriant sudėtingus, daugiamačius organizacinius ir valdymo reiškinius, kai svarbu atskleisti ne tik formalius procesus, bet ir neformalius sprendimų priėmimo mechanizmus, praktinius iššūkius bei institucinį kontekstą.

Ekspertinių interviu klausimynas buvo parengtas remiantis pirmojo ir antrojo disertacijos skyrių teorine analize bei suformuotu konceptualiu kibernetinio saugumo valdymo modeliu. Klausimai struktūruoti taip, kad apimtų pagrindines tyrimo dimensijas:

1. kibernetinio saugumo valdymo brandos lygį sveikatos sektoriaus organizacijose;
2. strateginio, organizacinio ir technologinio valdymo praktikas;
3. rizikų ir incidentų valdymo procesus;
4. atsakomybių pasiskirstymą ir informacijos srautų saugumą;

5. duomenų apsaugos ir pacientų saugos užtikrinimą e. sveikatos sistemose;
6. siūlomo kibernetinio saugumo valdymo modelio tinkamumą, pritaikomumą ir tobulinimo galimybes.

Toks klausimų struktūravimas užtikrino, kad surinkti empiriniai duomenys būtų tiesiogiai susieti su tyrimo uždaviniais, o ekspertų pateiktos įžvalgos galėtų būti sistemingai analizuojamos teminės analizės pagrindu.

Siekiant sustiprinti kokybinio tyrimo patikimumą ir užtikrinti duomenų triangulaciją, papildomai taikyta dokumentų analizė. Analizuoti strateginiai, norminiai ir metodiniai dokumentai, reglamentuojantys kibernetinį saugumą ir e. sveikatos sistemų veikimą, taip pat organizacijų vidaus politikos, gairės, viešai prieinamos ataskaitos ir rekomendacijos. Dokumentų analizė leido identifikuoti formalius reikalavimus, deklaruojamas praktikas ir jas palyginti su ekspertų pateikiamomis įžvalgomis, taip atskleidžiant galimus neatitikimus tarp normatyvinio reguliavimo ir realaus kibernetinio saugumo valdymo įgyvendinimo (Bowen, 2009).

Svarbus duomenų rinkimo proceso aspektas buvo tyrimo etikos laikymasis. Visi ekspertai buvo informuoti apie tyrimo tikslą, duomenų naudojimo pobūdį, anonimiškumo ir konfidencialumo užtikrinimą. Interviu duomenys buvo transkribuojami raštu ir analizuojami taip, kad nebūtų galima identifikuoti nei konkrečių asmenų, nei jų atstovaujamų institucijų. Tokia praktika atitinka mokslinių tyrimų etikos principus ir sudaro prielaidas atviram, refleksyviam bei patikimam ekspertų dalyvavimui tyrime (Kardelis, 2019).

Apibendrinant galima teigti, kad taikytos duomenų rinkimo priemonės – pusiau struktūrizuoti ekspertiniai interviu ir dokumentų analizė – sudaro nuoseklią ir metodologiškai pagrįstą sistemą, leidžiančią išsamiai atskleisti kibernetinio saugumo valdymo praktiką e. sveikatos sistemoje ir pagrįsti siūlomo valdymo modelio tikslinimo sprendinius. Šios priemonės sudaro pagrindą tolesnei empirinės medžiagos analizei, pateikiamai kitame disertacijos poskyryje.

2.4.5. Duomenų analizės metodai

Šiame disertaciniame tyrime taikyti duomenų analizės metodai parinkti atsižvelgiant į tyrimo tikslą, pasirinktą kokybinį tyrimo dizainą ir nagrinėjamo reiškinio – kibernetinio saugumo valdymo e. sveikatos sistemoje – kompleksiškumą. Kadangi tyrimas grindžiamas ekspertinių interviu duomenimis, pagrindinis dėmesys skiriamas kokybinei duomenų analizei, leidžiančiai atskleisti ekspertų patirties, vertinimų ir interpretacijų turinį bei jų tarpusavio sąsajas.

Pagrindiniu duomenų analizės metodu pasirinkta teminė analizė, kuri taikoma pusiau struktūrizuotų ekspertinių interviu analizei. Teminė analizė leidžia sistemingai identifikuoti pasikartojančias temas, esminius vienetus ir konceptualias kategorijas, atspindinčias ekspertų požiūrį į kibernetinio saugumo valdymo praktiką, brandą, spragas ir tobulinimo galimybes e. sveikatos sistemoje. Šis metodas yra plačiai taikomas informacinių sistemų, vadybos ir kibernetinio saugumo tyrimuose, kai siekiama analizuoti sudėtingus socio-techninius reiškinius (Tondel ir kt., 2014).

Duomenų analizės procesas buvo vykdomas nuosekliai, laikantis teminės analizės etapų logikos:

1. pirminė interviu analizė ir susipažinimas su duomenimis;
2. atvirasis kodavimas, identifikuojant esminius vienetus ir reikšmingus teiginius;
3. kodų grupavimas į aukštesnio lygmens temas ir analitines kategorijas;
4. temų peržiūra, siekiant užtikrinti jų vidinį nuoseklumą ir ryšį su tyrimo tikslais;
5. temų interpretacija ir integravimas į siūlomo kibernetinio saugumo valdymo modelio analizę.

Teminė analizė leido ne tik aprašyti ekspertų pateikiamas įžvalgas, bet ir interpretuoti jų reikšmę platesniame organizaciniame ir sisteminiame kontekste, atsižvelgiant į e. sveikatos sistemų specifiką, reguliacinę aplinką ir kritinį paslaugų pobūdį.

Svarbi analizės dalis buvo analitinė lyginamoji analizė, kurios metu ekspertų interviu metu identifikuotos praktikos, problemos ir spragos buvo lyginamos su teoriniais kibernetinio saugumo valdymo modeliais, tarptautiniais standartais ir brandos modeliais, aptartais pirmajame ir antrajame disertacijos skyriuose. Toks palyginimas leido įvertinti, kiek realioje praktikoje taikomi sprendimai atitinka normatyvinius reikalavimus ir gerąją praktiką, taip pat identifikuoti esminius neatitikimus, kurie tapo pagrindu siūlomo modelio tikslinimui (von Solms ir van Niekerk, 2018).

Duomenų interpretacijoje taikytas socio-techninis požiūris, pabrėžiantis technologinių, organizacinių, valdymo ir žmogiškųjų veiksnių tarpusavio sąveiką. Būtent toks integruotas interpretavimo požiūris yra būtinas vertinant kibernetinio saugumo brandą ir atsparumą kritinėse, griežtai reguliuojamose sistemose, tokiose kaip e. sveikatos infrastruktūra (Alshaikh, 2020; Sarker ir kt., 2019). Šis požiūris leido išvengti vienpusio technologinio vertinimo ir atskleisti sprendimų valdymo poveikį organizaciniam pasirengimui bei sistemos atsparumui.

Siekiant padidinti tyrimo patikimumą, taikyta duomenų trianguliacija, lyginant ekspertinių interviu metu gautas įžvalgas su dokumentų analizės rezultatais. Dokumentuose identifikuoti formaliai deklaruojami kibernetinio saugumo reikalavimai ir praktikos buvo interpretuojami ekspertų pateiktų vertinimų kontekste, leidžiant atskleisti atotrūkius tarp normatyvinio reguliavimo ir realaus įgyvendinimo (Bowen, 2009). Tokia trianguliacija sustiprino analizės pagrįstumą ir interpretacijų patikimumą.

Atsižvelgiant į tai, kad empirinis tyrimas grindžiamas kokybine ekspertinių interviu logika ir tikslingai atrinkta ekspertų imtimi, duomenų analizė organizuojama pagal disertacijoje suformuluotus tiriamuosius klausimus. Pagrindinis analizės metodas yra teminė ekspertinių interviu analizė, kurios metu ekspertų pasisakymai sisteminami į kategorijas ir subkategorijas, susijusias su kibernetinio saugumo valdymo fragmentiškumu, integruoto valdymo elementų taikymu, incidentų valdymo struktūrizuotumu ir siūlomo modelio galimu indėliu į organizacinį pasirengimą.

Kokybinės analizės metu buvo sudaromos kategorijų matricos, kuriose fiksuojama, kokios temos pasikartoja ekspertų pasisakymuose, kiek ekspertų jas mini ir kaip jos siejasi su disertacijoje suformuluotais tiriamaisiais klausimais. Toks analizės būdas leidžia identifikuoti pasikartojančius ekspertinių įžvalgų dėsningumus ir sistemiškai

atsakyti į tiriamuosius klausimus, nesiekiant statistinio rezultatų apibendrinimo visai populiacijai.

Papildomai ekspertų vertinimų suderinamumui įvertinti taikytas Kendall konkordacijos koeficientas W. Šis metodas šiame tyrime naudojamas kaip papildomas ekspertų nuomonių suderinamumo rodiklis, leidžiantis įvertinti, ar ekspertai panašiai vertina tuos pačius kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui kriterijus.

3. EMPIRINIO TYRIMO REZULTATAI IR KIBERNETINIO SAUGUMO VALDYMO MODELIO E. SVEIKATOS SISTEMOS TOBULINIMUI TIKSLINIMAS

Šiame disertacijos skyriuje pateikiami ir analizuojami empirinio tyrimo rezultatai, gauti taikant antrajame skyriuje pagrįstą kokybinio ekspertinio tyrimo metodologiją. Empirinis tyrimas orientuotas į sukurto kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui vertinimą, siekiant nustatyti jo tinkamumą, praktinį pritaikomumą bei identifikuoti tobulinimo kryptis realioje organizacinėje ir institucinėje aplinkoje.

Empiriniai duomenys buvo surinkti taikant pusiau struktūrizuotus ekspertinius interviu su kibernetinio saugumo ir e. sveikatos srities specialistais, turinčiais ilgametę patirtį strateginio, organizacinio ir technologinio saugumo valdymo srityse. Ekspertinis vertinimas leido atskleisti ne tik formaliai taikomas kibernetinio saugumo praktikas, bet ir giluminius sprendimų priėmimo, atsakomybės pasiskirstymo, informacijos srautų valdymo bei institucinių sąveikų aspektus, kurie yra kritiškai svarbūs e. sveikatos sistemų saugumui ir atsparumui.

Remiantis ekspertinio vertinimo duomenimis, šiame skyriuje nuosekliai analizuojamas esamas kibernetinio saugumo valdymo lygis sveikatos sektoriaus įstaigose, identifikuojamos esminės kibernetinio saugumo spragos, vertinamos rizikų ir incidentų valdymo praktikos bei nagrinėjama skirtingų valdymo lygių – strateginio, organizacinio ir technologinio – tarpusavio sąveika. Tokia analizė leidžia sistemiškai atsakyti į disertacijoje suformuluotus tiriamuosius klausimus ir įvertinti, kiek praktikoje taikomi sprendimai atitinka teorinius modelius, tarptautinius standartus ir gerąją praktiką.

Empiriniai rezultatai šiame skyriuje pateikiami struktūruotai, taikant teminės analizės principus ir sistemingai interpretuojant ekspertų pateiktas įžvalgas. Analizė grindžiama ekspertų citatomis, analitinėmis kategorijomis ir jų sąsajomis su siūlomo kibernetinio saugumo valdymo modelio komponentais. Toks analizės būdas užtikrina rezultatų analitinį ir interpretacinį nuoseklumą ir leidžia pagrįstai identifikuoti modelio stiprybes, ribotumus bei tobulinimo kryptis.

Šio skyriaus rezultatai sudaro empirinį pagrindą tolesniam kibernetinio saugumo valdymo modelio tikslinimui, pateikiamam vėlesniuose poskyriuose, bei leidžia suformuluoti moksliškai pagrįstas ir praktiškai reikšmingas rekomendacijas e. sveikatos sistemos kibernetinio saugumo valdymo stiprinimui.

3.1. Ekspertų nuomonės vertinimo tyrimo analizės struktūra

Šiame poskyryje pateikiama išsami empirinio tyrimo rezultatų analizė, grindžiama pusiau struktūrizuotų ekspertinių interviu metu surinktais kokybiniais duomenimis. Tyrimo rezultatų analizė orientuota į praktinį kibernetinio saugumo valdymo e. sveikatos sistemoje vertinimą, siekiant atskleisti esamą valdymo brandos lygį, identifikuoti kritines saugumo spragas bei įvertinti sukurto kibernetinio saugumo valdymo

modelio tinkamumą ir taikymo galimybes.

Empirinio tyrimo analizė struktūruojama nuosekliai, vadovaujantis kokybinio tyrimo ir teminės analizės logika, kai ekspertų pateiktos įžvalgos sisteminamos pagal iš anksto apibrėžtas analitines kategorijas, atitinkančias disertacijoje suformuoto kibernetinio saugumo valdymo modelio struktūrą. Tokia analizės eiga leidžia ne tik aprašyti pavienes ekspertų nuomones, bet ir atskleisti pasikartojančius dėsningumus, problemines sritis bei sisteminius iššūkius, būdingus e. sveikatos sistemų kibernetinio saugumo valdymui.

Pirmiausia pateikiamas ekspertų sociodemografinis ir profesinis profilis, leidžiantis gautas įžvalgas ir pagrįsti ekspertinio vertinimo patikimumą bei informacinę vertę. Toliau analizuojamas kibernetinio saugumo valdymo lygis sveikatos sektoriuje, identifikuojamos esminės kibernetinio saugumo spragos ir nagrinėjamos rizikų bei incidentų valdymo praktikos, remiantis ekspertų patirtimi ir vertinimais.

Tyrimo rezultatų analizė atliekama remiantis antrajame disertacijos skyriuje suformuoto kibernetinio saugumo valdymo modelio struktūra, vertinant strateginį, organizacinį, operacinį ir technologinį valdymo lygmenis bei jų tarpusavio sąveiką. Toks analitinis požiūris leidžia atskleisti ne tik atskirų saugumo priemonių ar procesų būklę, bet ir sisteminius kibernetinio saugumo valdymo iššūkius, susijusius su atsakomybės pasiskirstymu, informacijos srautais, sprendimų priėmimo praktika ir instituciniu koordinavimu e. sveikatos sistemoje.

3.1.1. Ekspertų sociodemografinis profilis

Siekiant užtikrinti empirinio tyrimo rezultatų patikimumą ir pagrįstą jų interpretavimą, būtina detaliai apibrėžti ekspertinio vertinimo dalyvių sociodemografinį ir profesinį profilį. Respondentų charakteristikų analizė leidžia įvertinti, ar tyrime dalyvavę ekspertai turi pakankamą kompetenciją, profesinę patirtį, būtiną kompleksiškai vertinti kibernetinio saugumo valdymą e. sveikatos sistemoje.

Kaip išdėstyta disertacijos 2.4.3 poskyryje, empirinio tyrimo imtį sudarė devyni kibernetinio saugumo srities ekspertai, atrinkti taikant tikslinę (ekspertinę) imties atranką. Visi respondentai turi reikšmingą profesinę patirtį kibernetinio saugumo, informacinių sistemų valdymo, viešojo sektoriaus informacinių sistemų ar sveikatos sektoriaus skaitmenizavimo srityse. Tokia ekspertų sudėtis sudaro prielaidas gauti argumentuotas ir tarpusavyje palyginamas įžvalgas apie kibernetinio saugumo valdymo praktiką e. sveikatos sistemoje.

Laikantis tyrimų etikos ir asmens duomenų apsaugos principų, respondentų anonimiškumas buvo užtikrintas suteikiant jiems identifikatorius (E1–E9). Apibendrintos ekspertų sociodemografinės ir profesinės charakteristikos pateikiamos 14 lentelėje.

14 lentelė. Respondentų sociodemografinės ir profesinės charakteristikos

Kriterijus	Charakteristikos	Respondentų skaičius
Lytis	Vyrai	6
	Moterys	3
Amžiaus grupė	30–39 m.	2
	40–49 m.	4
	50 m. ir daugiau	3
Profesinė patirtis kibernetinio saugumo srityje	5–9 metai	2
	10–14 metų	4
	15 metų ir daugiau	3
Pagrindinė profesinė veiklos sritis	Viešasis sektorius	4
	Sveikatos sektorius	2
	Kibernetinio saugumo institucijos	2
	Akademinė veikla	1
Dalyvavimas strateginiuose ar norminiuose procesuose	Nacionalinės strategijos, teisės aktų rengimas	6
	Organizacinės strategijos ir politikos	3
Išsilavinimas	Magistro laipsnis	7
	Daktaro laipsnis	2

Šaltinis: sudaryta autorės, remiantis ekspertinio interviu duomenimis

Analizuojant pateiktus duomenis, matyti, kad tyrime dalyvavę ekspertai pasižymi aukštu profesinės brandos lygiu. Dauguma respondentų turi ne mažesnę kaip dešimties metų darbo patirtį kibernetinio saugumo ar su juo glaudžiai susijusiose srityse, o tai ypač svarbu vertinant kompleksinius, sisteminius ir daugiasluoksnius reiškinius, tokius kaip kibernetinio saugumo valdymas e. sveikatos sistemoje. Reikšminga dalis ekspertų yra tiesiogiai dalyvavę nacionalinio lygmens strategijų, politikos dokumentų ar norminių aktų rengime ir įgyvendinime, todėl jų įžvalgos apima ne tik organizacinį, bet ir valstybės kibernetinio saugumo valdymo požiūrį.

Ekspertų profesinių veiklų įvairovė, apimanti viešojo sektoriaus institucijas, sveikatos sektoriaus įstaigas, akademinę bendruomenę, sudaro prielaidas palyginti skirtingus požiūrius ir sumažinti vienos institucinės perspektyvos dominavimo riziką. Tokia imties struktūra didina ekspertinio vertinimo rezultatų analitinį patikimumą ir leidžia juos laikyti tinkamais nagrinėjamos problematikos kontekste.

Apibendrinant galima teigti, kad tyrime dalyvavusių ekspertų sociodemografinės ir profesinės charakteristikos atitinka disertacinio lygmens empiriniams tyrimams keliamus reikalavimus ir sudaro pagrindą tolesnei kibernetinio saugumo valdymo lygio, spragų ir tobulinimo galimybių analizei, kuri plėtojama kituose 3.1. skyriaus poskyriuose.

3.1.2. Kibernetinio saugumo valdymo lygio vertinimas sveikatos įstaigose ekspertų požiūriu

Vertinant dabartinį kibernetinio saugumo valdymo lygį sveikatos įstaigose, šiame disertaciniame tyrime buvo remtasi pusiau struktūruotų interviu su kibernetinio saugumo srities ekspertais duomenimis. Ekspertų patirtys ir įžvalgos leido atskleisti faktinę kibernetinio saugumo būklę e. sveikatos sistemoje ne tik formaliu, bet ir praktiniu lygmeniu, atsižvelgiant į strateginius, organizacinius, technologinius ir žmogiškuosius veiksnius.

Ekspertų vertinimu, dabartinis kibernetinio saugumo lygis sveikatos sektoriuje negali būti laikomas nuosekliu visos sistemos mastu. Priešingai, jis pasižymi ryškiu fragmentiškumu, nevienodu brandos lygiu ir didele priklausomybe nuo individualių institucijų iniciatyvų bei vadovybės požiūrio.

Vienas ekspertas situaciją apibūdino taip:

„Negalima sakyti, kad e. sveikatos sistema kaip visuma yra saugi arba nesaugi. Realiai matome labai skirtingus lygius, nuo gana pažangių sprendimų iki visiškai bazinio saugumo“ (E1, asmeninis interviu, 2024-07-08).

Analizuojant ekspertų atsakymus išryškėjo, kad vienas esminių veiksnių, lemiančių dabartinį kibernetinio saugumo lygį, yra strateginio saugumo suvokimo stoka organizacijų vadovybės lygmeniu. Nors kibernetinis saugumas dažnai formaliai įtraukiamas į strateginius dokumentus, praktikoje jis ne visada suvokiamas kaip integrali organizacijos veiklos ir rizikų valdymo dalis.

„Daugelyje sveikatos įstaigų saugumas vis dar suvokiamas kaip informacinių technologijų klausimas, o ne kaip organizacinė ar strateginė rizika“ (E9, asmeninis interviu, 2024-07-25).

Ekspertai pabrėžė, kad tokia nuostata lemia fragmentiškus, dažnai neapgalvotus sprendimus, kai kibernetinis saugumas tampa prioritetu tik po reikšmingų sutrikimų ar incidentų:

„Kol neįvyksta rimtas incidentas, saugumas lieka antrame plane. Tik po sutrikimų atsiranda supratimas, kad reikėjo investuoti anksčiau“ (E4, asmeninis interviu, 2024-07-15).

Tai leidžia teigti, kad dabartinis saugumo lygis daugelyje sveikatos įstaigų yra grindžiamas reagavimu į įvykius, o ne sisteminga prevencine strategija, kuri yra būdinga aukštesnės brandos kibernetinio saugumo valdymo sistemoms.

Ekspertai taip pat išsamiai vertino rizikų valdymo procesus sveikatos įstaigose. Nors formaliai rizikų vertinimas dažnai atliekamas, jo rezultatai ne visada integruojami į kasdienius valdymo ir sprendimų priėmimo procesus.

„Rizikų analizės dokumentai egzistuoja, bet jie dažnai neatnaujinami ir nenaudojami realiems sprendimams“ (E6, asmeninis interviu, 2024-07-18).

Kai kurie ekspertai pabrėžė ir formalų požiūrį į rizikų vertinimą:

„Rizikos identifikuojamos tam, kad būtų atitikti reglamentų reikalavimai, bet ne tam, kad būtų realiai valdomos“ (E2, asmeninis interviu, 2024-07-09).

Panašios tendencijos pastebėtos ir incidentų valdymo srityje. Nors daugelyje

organizacijų egzistuoja incidentų valdymo planai, jų praktinis taikymas ir testavimas yra ribotas:

„Planai yra, bet realaus pasirengimo dažnai trūksta. Incidento metu pasimato, kad nėra aišku, kas už ką atsakingas“ (E7, asmeninis interviu, 2024-07-22).

Be to, ekspertai akcentavo organizacinio mokymosi stoką po incidentų:

„Po incidentų retai atliekama gilesnė analizė. Dažniausiai svarbu kuo greičiau atstatyti veiklą, bet nepasimokoma ateičiai“ (E8, asmeninis interviu, 2024-07-23).

Tai rodo, kad dabartinis incidentų valdymo lygis dažnai neužtikrina ilgalaikio organizacijų atsparumo ir nuoseklaus saugumo brandos augimo.

Ekspertų vertinimu, technologinis saugumas sveikatos įstaigose yra vienas labiausiai išvystytų, tačiau kartu ir labiausiai netolygiai taikomų elementų. Didesnės organizacijos dažniau investuoja į pažangias technologines priemones, tuo tarpu mažesnės įstaigos dažnai apsiriboja baziniais sprendimais:

„Technologijų lygis labai skiriasi. Kai kur matome modernias stebėsenos sistemas, kitur – pasenusią infrastruktūrą“ (E3, asmeninis interviu, 2024-07-11).

Taip pat buvo akcentuota, kad technologijos neretai diegiamos fragmentiškai, be bendros architektūrinės ir valdymo vizijos:

„Techninės priemonės diegiamos fragmentiškai, be aiškios bendros architektūros ar saugumo vizijos“ (E5, asmeninis interviu, 2024-07-16).

Žmogiškasis veiksnys ekspertų vertinimu išlieka viena silpniausių kibernetinio saugumo grandžių. Darbuotojų sąmoningumo, kompetencijų ir saugumo kultūros stoka tiesiogiai veikia faktinį saugumo lygį:

„Didžiausia problema dažnai nėra technologijos, o žmonės. Klaidos, neatsargumas ir laiko trūkumas daro didelę įtaką saugumui“ (E5, asmeninis interviu, 2024-07-16).

„Saugumo kultūra dar tik formuojasi. Daugeliui darbuotojų saugumas nėra prioritetas, nes jie orientuoti į savo darbo užduotis“ (E7, asmeninis interviu, 2024-07-22).

Tai leidžia teigti, kad dabartinis kibernetinio saugumo lygis sveikatos įstaigose yra neatsiejamas nuo organizacinės kultūros ir žmogiškųjų išteklių brandos.

Apibendrinant ekspertų interviu analizę, galima teigti, kad dabartinis kibernetinio saugumo valdymo lygis sveikatos įstaigose yra nevienalytis, fragmentuotas ir dažniausiai reaktyvus. Nors egzistuoja atskiri technologiniai ir organizaciniai sprendimai, jie nėra integruoti į vientisą, brandos principais grįstą kibernetinio saugumo valdymo sistemą.

Ekspertų įžvalgos rodo, kad toks saugumo lygis neužtikrina pakankamo atsparumo kibernetinėms grėsmėms ir sudaro prielaidas sisteminėms spragoms. Šios išvados sudaro empirinį pagrindą kitame poskyryje pereiti prie detalesnės kibernetinio saugumo spragų identifikavimo analizės, kuri leis struktūruotai įvertinti silpnąsias vietas ir pagrįsti siūlomo kibernetinio saugumo valdymo modelio tikslinimo kryptis.

3.1.3. Kibernetinio saugumo spragų identifikavimas e. sveikatos sistemoje ekspertų požiūriu

Atlikus dabartinio kibernetinio saugumo valdymo lygio vertinimą sveikatos įstaigose, kitas empirinio tyrimo etapas buvo skirtas sistemingai identifikuoti esmines

kibernetinio saugumo spragas, kurios riboja e. sveikatos sistemos atsparumą kibernetinėms grėsmėms ir trukdo efektyviam saugumo valdymui. Ši analizė grindžiama pusiau struktūruotų ekspertinių interviu duomenimis ir orientuota ne į pavienių techninių trūkumų fiksavimą, bet į gilesnių, struktūrinių ir organizacinių silpnųjų vietų atskleidimą.

Ekspertų atsakymai atskleidė, kad kibernetinio saugumo spragos sveikatos sektoriuje yra daugiasluoksnės, tarpusavyje susijusios ir sisteminės, dažnai viena kitą stiprinančios. Dėl šios priežasties spragų analizė struktūruojama pagal pagrindines analitines kategorijas: strateginio valdymo, organizacinės struktūros ir atsakomybių, rizikų ir incidentų valdymo, technologinio saugumo, žmogiškojo veiksnio bei tarpinstitucinio koordinavimo spragas.

Viena ryškiausių ekspertų identifikuotų spragų yra strateginio kibernetinio saugumo valdymo stoka. Ekspertų nuomone, daugelyje sveikatos įstaigų kibernetinis saugumas nėra sistemiškai integruotas į bendrą organizacijos strategiją, o dažnai egzistuoja kaip atskira, izoliuota funkcija.

„Saugumas dažnai nėra strateginis prioritetas. Jis atsiranda dokumentuose, bet ne realiuose sprendimuose“ (E1, asmeninis interviu, 2024-07-08).

Ilgalaikės vizijos ir nuoseklaus planavimo stoka lemia trumpalaikius, fragmentuotus sprendimus:

„Nėra aiškios ilgalaikės vizijos, kaip turėtų atrodyti saugumo sistema po penkerių metų. Viskas sprendžiama trumpalaikiais projektais“ (E4, asmeninis interviu, 2024-07-15).

Šios spragos rodo, kad kibernetinis saugumas dažnai nėra suvokiamas kaip organizacijos atsparumo ir veiklos tęstinumo dalis, o tai būdinga žemesnio brandos lygio saugumo valdymo sistemoms.

Kita reikšminga spragų grupė susijusi su neaiškiu organizaciniu kibernetinio saugumo valdymu ir atsakomybių paskirstymu. Ekspertai pažymėjo, kad atsakomybės dažnai yra išskaidytos, persidengiančios arba neformalizuotos.

„Nėra aišku, kas atsakingas už saugumą – IT skyrius, vadovybė ar išorinis tiekėjas“ (E7, asmeninis interviu, 2024-07-22).

„Kai atsakomybė išskaidyta, realiai ji tampa niekieno“ (E2, asmeninis interviu, 2024-07-09).

Tokios organizacinės spragos apsunkina koordinuotą sprendimų priėmimą, lėtina reagavimą į incidentus ir mažina visos sistemos atsparumą. Ekspertų vertinimu, aiškios atsakomybės nebuvimas yra viena iš pagrindinių priežasčių, kodėl saugumo sprendimai nepasiekia operacinio lygmens.

Ekspertų interviu atskleidė, kad rizikų valdymas dažnai yra viena silpniausių kibernetinio saugumo valdymo sričių. Nors rizikų identifikavimas ir vertinimas formaliai atliekamas, jis dažnai netampa realių sprendimų pagrindu.

„Rizikos identifikuojamos, bet jų valdymas dažnai lieka teorinis“ (E6, asmeninis interviu, 2024-07-18).

Ekspertai pabrėžė ir prioretizavimo problemą:

„Ne visos rizikos yra vienodai pavojingos, bet tai dažnai neatsispindi valdymo

sprendimuose“ (E9, asmeninis interviu, 2024-07-25).

Dėl šių spragų resursai paskirstomi neproporcingai, o kritinės rizikos gali likti nepakankamai valdomos, kas didina didelio poveikio incidentų tikimybę.

Analizuojant incidentų valdymo praktiką, išryškėjo atotrūkis tarp formalių planų ir realaus pasirengimo. Ekspertai pažymėjo, kad incidentų valdymo procedūros dažnai nėra testuojamos ar integruotos į kasdienę veiklą.

„Kai įvyksta incidentas, paaiškėja, kad planas neveikia taip, kaip tikėtasi“ (E8, asmeninis interviu, 2024-07-23).

Taip pat akcentuotas sisteminio mokymosi po incidentų trūkumas:

„Po incidento svarbiausia atkurti sistemas, bet retai analizuojama, kodėl tai įvyko“ (E5, asmeninis interviu, 2024-07-16).

Tai rodo, kad incidentų valdymas dažnai nėra suvokiamas kaip nuolatinio tobulinimo ciklo dalis.

Technologinės spragos, ekspertų vertinimu, dažniausiai kyla ne dėl priemonių nebuvimo, o dėl jų fragmentiško diegimo, nepakankamos integracijos ir pasenusios infrastruktūros.

„Techninių sprendimų yra daug, bet jie neveikia kaip vientisa sistema“ (E3, asmeninis interviu, 2024-07-11).

„Kai kurios sistemos yra pasenusios, bet jų keitimas atidedamas dėl lėšų trūkumo“ (E6, asmeninis interviu, 2024-07-18).

Tokios spragos didina atakos paviršių ir apsunkina centralizuotą saugumo valdymą.

Žmogiškasis veiksnys ekspertų buvo įvardytas kaip viena didžiausių sisteminių spragų. Nepakankamas darbuotojų sąmoningumas ir formalūs mokymai neleidžia formuoti tvarios saugumo kultūros.

„Net ir geriausios technologijos nepadės, jei žmonės nesupranta saugumo svarbos“ (E5, asmeninis interviu, 2024-07-16).

„Mokymai vyksta, bet jie dažnai formalūs ir neorientuoti į realias grėsmes“ (E7, asmeninis interviu, 2024-07-22).

Ekspertų nuomone, reikšminga spragų grupė susijusi su tarpinstituciniu koordinavimu. E. sveikatos sistema veikia kaip tarpusavyje priklausoma ekosistema, kurioje vienos organizacijos pažeidžiamumas gali turėti sisteminių pasekmių.

„Vienos įstaigos saugumo spraga gali paveikti visą sistemą“ (E1, asmeninis interviu, 2024-07-08).

„Trūksta bendrų standartų ir koordinuoto reagavimo tarp institucijų“ (E9, asmeninis interviu, 2024-07-25).

Apibendrinant galima teigti, kad identifikuotos kibernetinio saugumo spragos e. sveikatos sistemoje yra kompleksinės, tarpusavyje susijusios ir apimančios visus valdymo lygmenis – nuo strateginio iki žmogiškojo. Šios spragos lemia fragmentuotą, nepakankamai koordinuotą ir dažnai reaktyvų kibernetinio saugumo valdymą.

Identifikuotos spragos nukreipia kitame poskyryje pereiti prie rizikų ir incidentų valdymo praktikos vertinimo, kuris leis įvertinti, kaip šios spragos pasireiškia praktikoje ir kokiu mastu siūlomas kibernetinio saugumo valdymo modelis gali prisidėti prie e. sveikatos sistemos atsparumo didinimo.

3.1.4. Rizikų ir incidentų valdymo praktikos vertinimas ekspertų požiūriu

Šiame poskyryje analizuojamas praktinis kibernetinių rizikų ir incidentų valdymo veiksmingumas sveikatos sektoriaus įstaigose, remiantis pusiau struktūruotų ekspertinių interviu duomenimis. Skirtingai nei ankstesniuose poskyriuose, kuriuose buvo apibrėžtas bendras kibernetinio saugumo valdymo lygis ir identifikuotos sisteminės spragos, ši analizė orientuota į tai, kaip realiai veikia rizikų valdymo ir incidentų valdymo procesai, kiek jie yra integruoti į organizacinį valdymą, kokie mechanizmai užtikrina (ar neužtikrina) grįžtamąjį ryšį ir mokymąsi, bei kaip tai veikia e. sveikatos sistemos atsparumą.

Ekspertų vertinimu, rizikų ir incidentų valdymas sveikatos sektoriuje dažnai egzistuoja kaip formaliai apibrėžta veikla, tačiau praktinis jos veiksmingumas yra nevienodas ir priklauso nuo institucinių, žmogiškųjų bei technologinių veiksnių. Tai reiškia, kad vienose organizacijose rizikos ir incidentai valdomi sistemiškai, o kitose – fragmentiškai, epizodiškai arba reaguojant tik į išorinius reikalavimus.

Ekspertai pažymėjo, kad rizikų identifikavimas sveikatos įstaigose dažniausiai vykdomas dokumentiniu lygmeniu, tačiau ne visada apima visą galimų grėsmių spektrą. Rizikos dažnai įvardijamos reaguojant į auditą, patikrinimą ar jau įvykusį incidentą, o ne nuolatos.

„Rizikos dažniausiai identifikuojamos tada, kai to reikalauja auditas arba po realaus incidento“ (E3, asmeninis interviu, 2024-07-11).

Ekspertai akcentavo, kad identifikavimo praktika neretai apsiriboja techninėmis grėsmėmis, kai tuo tarpu organizaciniai ir žmogiškieji veiksniai lieka nepakankamai įvertinti.

„Didžiausias dėmesys skiriamas techninėms rizikoms, bet organizacinės ir žmogiškosios dažnai lieka paraštėse“ (E6, asmeninis interviu, 2024-07-18).

Tai rodo, kad rizikų identifikavimas ne visada atspindi socio-techninę e. sveikatos sistemų prigimtį, kur technologinė priklausomybė persipina su procesais, darbo organizavimu, paslaugų teikimo logika ir pacientų saugos reikalavimais.

Ekspertų atsakymai atskleidė, kad net ir identifikavus rizikas, jų analizė dažnai atliekama paviršutiniškai, apsiribojant bendrais apibūdinimais („aukšta“, „vidutinė“), tačiau neįvertinant konkretaus poveikio klinikiniams procesams, pacientų saugai ir paslaugų tęstinumui.

„Rizika įvertinama kaip „aukšta“ arba „vidutinė“, bet retai nagrinėjama, ką tai reiškia realiai paslaugų teikimui“ (E8, asmeninis interviu, 2024-07-23).

Taip pat išryškėjo aiškaus prioretizavimo mechanizmo stoka, kai organizacijos neturi nuoseklių kriterijų, pagal kuriuos rizikoms būtų skiriamas dėmesys, resursai ir kontrolė.

„Visos rizikos atrodo svarbios, bet nėra aiškaus mechanizmo, kurioms skirti daugiausia dėmesio“ (E2, asmeninis interviu, 2024-07-09).

Šios įžvalgos leidžia teigti, kad rizikų analizė dažnai nėra pakankamai susieta su sprendimų priėmimu, rizikų dokumentacija egzistuoja, tačiau jų turinys ne visada tampa realiu pagrindu prioritetams, biudžeto poreikiui pagrįsti, pokyčių planams ar kontrolės stiprinimui.

Ekspertai nurodė, kad rizikų mažinimo priemonės dažnai pasirenkamos remiantis techninių sprendimų prieinamumu, projekto patogumu ar finansavimo galimybėmis, tačiau ne sisteminiu rizikos poveikio vertinimu. Tai lemia fragmentuotą priemonių diegimą ir netolygų rizikų mažinimo efektą.

„Diegiamos tos priemonės, kurios lengviausiai įgyvendinamos, bet nebūtinai tos, kurios labiausiai sumažina riziką“ (E5, asmeninis interviu, 2024-07-16).

„Trūksta aiškaus ryšio tarp nustatytos rizikos ir konkretaus valdymo sprendimo“ (E1, asmeninis interviu, 2024-07-08).

Praktikoje tai reiškia, kad rizikos valdymo veikla gali virsti atskirų priemonių kolekcionavimu, kai organizacija turi įvairių saugumo sprendimų, bet jie nėra integruoti į kryptingą rizikų mažinimo programą.

Vienas svarbiausių rizikų valdymo efektyvumo kriterijų yra jo integracija į organizacijos valdymą. Ekspertų nuomone, sveikatos sektoriuje rizikų valdymas dažnai lieka informacinių technologijų skyriaus ar saugumo specialistų atsakomybės dalis ir nepakankamai pasiekia strateginį sprendimų priėmimo lygmenį.

„Rizikų valdymas dažniausiai lieka IT arba saugumo specialistų atsakomybė“ (E7, asmeninis interviu, 2024-07-22).

Vadovybės įsitraukimas, ekspertų teigimu, yra esminė sąlyga, kad rizikų valdymas iš „popierinės“ praktikos taptų veikiančiu valdymo mechanizmu.

„Jei vadovybė aktyviai nesidomi rizikomis, jos lieka popieriuje“ (E4, asmeninis interviu, 2024-07-15).

Tai atskleidžia, kad rizikų valdymo brandą dažnai lemia ne vien metodika, o sprendimų kultūra, ar rizikos suvokiamos kaip strateginės, ar laikomos tik techniniu klausimu.

Ekspertų teigimu, rizikų stebėsena ir periodinė peržiūra dažnai vykdoma nereguliariai, o tai lemia, kad rizikų valdymo procesas tampa statiškas ir neadekvatus sparčiai kintančiai grėsmių aplinkai.

„Rizikų sąrašas atnaujinamas kartą per metus, bet grėsmės keičiasi greičiau“ (E9, asmeninis interviu, 2024-07-25).

Be to, išryškėjo grįžtamojo ryšio trūkumas, ne visada pasimokoma per incidentus.

„Nėra aiškaus mechanizmo, kaip pamokos iš incidentų būtų grąžinamos į rizikų valdymą“ (E3, asmeninis interviu, 2024-07-11).

Tai leidžia daryti išvadą, kad rizikų valdymo ciklas dažnai nėra uždaromas, o organizacijos praranda galimybę nuosekliai didinti brandą remiantis realiais įvykiais.

Vertinant incidentų valdymą, ekspertai akcentavo, kad formaliai incidentų valdymo planai ar procedūros dažnai būna parengti, tačiau praktinis jų veikimas priklauso nuo organizacinės disciplinos, atsakomybių aiškumo ir testavimo (pratybų) kultūros. Kitaip tariant, incidentų valdymas egzistuoja kaip dokumentas, bet ne visada kaip veiksmas.

Ekspertų požiūriu, vienas kritiškiausių aspektų yra koordinavimo ir komunikacijos spragos incidento metu, net ir turint formalius aprašus, realioje situacijoje atsiskleidžia, kad darbuotojai nežino, kas priima sprendimus, kam pranešti, kokia eskalavimo grandinė.

Nors šiame poskyryje daugiausia dėmesio skiriama rizikų valdymui, ekspertų

įžvalgos leidžia teigti, kad incidentų valdymo brandą tiesiogiai riboja tos pačios sisteminės problemos: atsakomybių neaiškumas, ribotas testavimas, fragmentuota stebėsena ir silpnas organizacinis mokymasis.

Apibendrinant ekspertų vertinimus galima teigti, kad rizikų ir incidentų valdymo praktika sveikatos sektoriaus organizacijose yra ribota ir nenuosekli. Nors pagrindiniai procesai formaliai egzistuoja, jų praktinis poveikis kibernetinio saugumo stiprinimui dažnai yra nepakankamas, nes:

1. rizikų identifikavimas ir analizė neretai išlieka dokumentinio pobūdžio,
2. mažinimo priemonės pasirenkamos ne visada pagal didžiausią poveikį,
3. rizikų valdymas nepakankamai integruotas į vadovybės sprendimų priėmimą,
4. stebėsena ir grįžtamasis ryšys iš incidentų dažnai neuždaro rizikų valdymo ciklo.

Šios įžvalgos patvirtina, kad esminė problema nėra pavienių saugumo priemonių trūkumas, bet sisteminis rizikų ir incidentų valdymo nebrandumas, ribojantis e. sveikatos sistemos atsparumą.

3.2. Teminė ekspertinė interviu analizė

Šiame disertacijos skyriuje pateikiama teminė ekspertinių interviu analizė, kurios tikslas – struktūruotai ir interpretuojamai atskleisti pagrindines kibernetinio saugumo valdymo problemas, dėsningumus ir požiūrių skirtumus e. sveikatos sistemos kontekste. Skirtingai nei ankstesniame 3.1 skyriuje, kuriame empiriniai duomenys buvo analizuojami aprašomuoju ir lyginamuoju aspektu, šiame skyriuje atliekama gilesnė analitinė interpretacija, orientuota į prasminių temų, pasikartojančių naratyvų ir struktūrinių sąsajų identifikavimą.

Teminė analizė leidžia pereiti nuo pavienių ekspertų pasisakymų prie konceptualizuotų analitinių kategorijų, kurios atspindi ne tik individualią patirtį, bet ir sistemines e. sveikatos kibernetinio saugumo valdymo tendencijas. Šis metodas ypač tinkamas tiriant sudėtingus socio-techninius reiškinius, kuriuose technologiniai sprendimai yra glaudžiai susiję su organizacine kultūra, valdymo struktūromis, teisiniu reguliavimu ir žmogiškaisiais veiksniais.

Teminė analizė šiame tyrime grindžiama indukciniu – dedukciniu principu, analitinės temos formuojamos remiantis tiek teorinėmis prielaidomis, išplėtotomis pirmajame ir antrajame disertacijos skyriuose, tiek empiriniais duomenimis, išryškėjusiais ekspertinių interviu metu. Toks požiūris leidžia ne tik patvirtinti teorijoje identifikuotas problemas, bet ir atskleisti naujus, literatūroje mažiau akcentuojamus aspektus, būdingus būtent e. sveikatos sistemos kibernetinio saugumo kontekstui.

Šiame skyriuje ekspertų pateiktos įžvalgos analizuojamos pagal pagrindines teminės kryptis, atspindinčias skirtingus kibernetinio saugumo valdymo lygmenis: strateginį ir organizacinį valdymą, technologinių sprendimų ir procesų brandą, taip pat teisinio reguliavimo ir praktinio įgyvendinimo sąveiką. Tokia analizės struktūra leidžia sistemiškai įvertinti, kaip skirtingi valdymo lygiai tarpusavyje sąveikauja, kur susiformuoja didžiausi neatitikimai ir kaip jie veikia bendrą e. sveikatos sistemos atsparumą kibernetinėms grėsmėms.

Teminės ekspertinių interviu analizės rezultatai šiame skyriuje sudaro pagrindą vėlesniam siūlomo kibernetinio saugumo valdymo modelio tikslinimui. Identifikuotos temos ir jų tarpusavio sąsajos leidžia pereiti nuo problemų konstatavimo prie struktūruotų, empiriškai pagrįstų sprendimų formavimo, kurie plėtojami 3.3 skyriuje, integruojant ekspertų įžvalgas į kibernetinio saugumo valdymo modelio struktūrą ir funkcinius komponentus.

Siekiant sistemingai apibendrinti ekspertinių interviu metu gautus duomenis ir užtikrinti analitinį nuoseklumą, buvo atlikta teminė analizė, kurios rezultatai struktūruotai pateikiami 15 lentelėje. Lentelėje identifikuotos pagrindinės kibernetinio saugumo valdymo problemų temos, išryškėjusios ekspertų atsakymuose, ir pateikiamos jas pagrindžiančios empirinės citatos. Ši lentelė sudaro analitinį pagrindą tolesniems 3.2 skyriaus poskyriams, kuriuose kiekviena tema nagrinėjama detaliau.

15 lentelė. Teminė ekspertinių interviu analizė

Analitinė tema	Identifikuota problema	Ekspertų citatos, pagrindžiančios problemą
Strateginis kibernetinio saugumo valdymas	Kibernetinio saugumo strateginis formalumas	„Kibernetinis saugumas yra paminėtas strateginiuose dokumentuose, bet realiai jis neturi tokio svorio kaip finansai ar veiklos rodikliai“ (1E, asmeninis interviu, 2024-07-08). „Strategijoje saugumas yra, bet sprendimų priėmime jis dažnai dingsta“ (4E, asmeninis interviu, 2024-07-15). „Tai labiau deklaracija nei reali strateginė kryptis“ (9E, asmeninis interviu, 2024-07-25).
	Reaktyvus vadovybės požiūris	„Vadovybė saugumu pradeda domėtis tada, kai jau įvyko incidentas“ (2E, asmeninis interviu, 2024-07-09). „Kol sistema veikia, saugumas atrodo kaip teorinis klausimas“ (4E, asmeninis interviu, 2024-07-15). „Prevencija dažnai laikoma per brangia, kol neatsitinka problema“ (6E, asmeninis interviu, 2024-07-18).
Organizacinė struktūra ir atsakomybės	Neaiškus atsakomybės pasiskirstymas	„Nėra vieno aiškaus atsakingo asmens už kibernetinį saugumą“ (7E, asmeninis interviu, 2024-07-22). „Atsakomybė paskirstyta taip, kad galiausiai niekas nesijaučia atsakingas“ (2E, asmeninis interviu, 2024-07-09). „Incidento metu visi laukia, kas ims iniciatyvą“ (8E, asmeninis interviu, 2024-07-23).
	Saugumo funkcijų priskyrimas IT padaliniui	„Saugumas vis dar suvokiamas kaip IT skyriaus problema“ (5E, asmeninis interviu, 2024-07-16). „Vadovybė dažnai nusišalina, nes mano, kad tai techninis klausimas“ (9E, asmeninis interviu, 2024-07-25). „Organizaciniai aspektai lieka nuošalyje“ (3E, asmeninis interviu, 2024-07-11).

Analitinė tema	Identifikuota problema	Ekspertų citatos, pagrindžiančios problemą
Rizikų valdymo praktika	Formalus rizikų identifikavimas	„Rizikos identifikuojamos tam, kad būtų dokumentuotos“ (3E, asmeninis interviu, 2024-07-11). „Tai daroma labiau dėl audito, o ne dėl realaus valdymo“ (6E, asmeninis interviu, 2024-07-18). „Praktikoje rizikos gyvena atskirai nuo sprendimų“ (1E, asmeninis interviu, 2024-07-08).
	Nepakankamas rizikų prioretizavimas	„Visos rizikos atrodo vienodai svarbios“ (2E, asmeninis interviu, 2024-07-09). „Nėra aišku, kuri rizika kritinė, o kuri – toleruotina“ (8E, asmeninis interviu, 2024-07-23). „Resursai paskirstomi ne pagal riziką, o pagal galimybes“ (5E, asmeninis interviu, 2024-07-16).
Incidentų valdymas	„Popierinis“ pasirengimas incidentams	„Planai egzistuoja, bet realiai jie nėra išbandyti“ (7E, asmeninis interviu, 2024-07-22). „Incidento metu paaiškėja, kad planas buvo teorinis“ (8E, asmeninis interviu, 2024-07-23). „Pratybos vyksta labai retai arba visai nevyksta“ (4E, asmeninis interviu, 2024-07-15).
	Organizacinio mokymosi stoka	„Po incidento svarbiausia atkurti veiklą, o ne mokytis“ (5E, asmeninis interviu, 2024-07-16). „Pamokos dažnai lieka neformalios ir neužfiksuotos“ (9E, asmeninis interviu, 2024-07-25). „Klaidos kartojasi, nes nėra sisteminio grįžtamojo ryšio“ (3E, asmeninis interviu, 2024-07-11).
Technologinis saugumas	Fragmentuota technologinė architektūra	„Technologijos diegiamos atskirai, be bendros architektūros“ (3E, asmeninis interviu, 2024-07-11). „Kiekviena sistema saugoma savaip“ (6E, asmeninis interviu, 2024-07-18). „Nėra centralizuoto saugumo vaizdo“ (1E, asmeninis interviu, 2024-07-08).
	Techninė skola	„Pasenusios sistemos kelia didžiausią riziką“ (6E, asmeninis interviu, 2024-07-18). „Jų keitimas nuolat atidedamas dėl kaštų“ (4E, asmeninis interviu, 2024-07-15). „Tai tiksinti bomba“ (2E, asmeninis interviu, 2024-07-09).
Žmogiškasis veiksnys	Silpna saugumo kultūra	„Saugumas darbuotojams dažnai nėra prioritetas“ (7E, asmeninis interviu, 2024-07-22). „Klinikiniai procesai visada svarbesni už saugumą“ (5E, asmeninis interviu, 2024-07-16). „Žmonės saugumą mato kaip trukdį“ (9E, asmeninis interviu, 2024-07-25).
	Formalūs mokymai	„Mokymai vyksta, bet jie neatspindi realių grėsmių“ (2E, asmeninis interviu, 2024-07-09). „Darbuotojai nežino, kaip elgtis realaus incidento metu“ (8E, asmeninis interviu, 2024-07-23). „Tai daugiau formalumas nei realus pasirengimas“ (6E, asmeninis interviu, 2024-07-18).
Tarpinstitucinis lygmuo	Sisteminė priklausomybė ir koordinavimo stoka	„Vienos įstaigos spraga gali paveikti visą sistemą“ (1E, asmeninis interviu, 2024-07-08). „Nėra bendro koordinuoto reagavimo mechanizmo“ (9E, asmeninis interviu, 2024-07-25). „Institucijos veikia atskirai, o ne kaip sistema“ (3E, asmeninis interviu, 2024-07-11).

Šaltinis: sudaryta autorės, remiantis ekspertinio tyrimo rezultatais

Ekspertų citatos rodo ne tik atskirų organizacijų praktikos trūkumus, bet ir gilesnę valdymo problemą. Kibernetinis saugumas dažnai yra formaliai įtrauktas į strateginius dokumentus, tačiau netampa realiu sprendimų priėmimo kriterijumi. Tai reiškia, kad modelyje nepakanka numatyti strateginio lygmens egzistavimo. Būtina parodyti, kaip strateginiai tikslai transformuojami į atsakomybę, biudžeto planavimą, rizikų prioritetus ir operacines procedūras. Būtent šis strategijos ir praktikos atotrūkis turėtų būti vienas pagrindinių modelio tikslinimo argumentų.

3.2.1. Strateginio ir organizacinio valdymo problematika

Teminė ekspertinių interviu analizė atskleidė, kad strateginio ir organizacinio kibernetinio saugumo valdymo problematika e. sveikatos sistemoje yra viena esminių priežasčių, lemiančių bendrą sistemos pažeidžiamumą ir nepakankamą atsparumą kibernetinėms grėsmėms. Ekspertų vertinimu, technologinės priemonės, teisinis reguliavimas ir pavieniai organizaciniai sprendimai negali užtikrinti veiksmingo saugumo, jeigu jie nėra integruoti į nuoseklią strateginę ir organizacinę valdymo sistemą.

Analizuojant ekspertų interviu atsakymus tapo akivaizdu, kad strateginio ir organizacinio lygmens spragos veikia kaip didinantys kitų saugumo trūkumų poveikį. Net ir esant pakankamam technologiniam lygiui ar formaliai atitinkant reguliacinius reikalavimus, strateginio koordinavimo ir aiškios organizacinės struktūros stoka lemia fragmentuotą, reaktyvų ir trumpalaikiais sprendimais grindžiamą kibernetinio saugumo valdymą.

Vienas dažniausiai ekspertų minimų aspektų – nepakankama kibernetinio saugumo integracija į organizacijos strateginį valdymą. Ekspertų nuomone, daugelyje sveikatos sektoriaus organizacijų kibernetinis saugumas egzistuoja kaip atskira funkcija, tačiau nėra suvokiamas kaip strateginis veiksnys, turintis tiesioginę įtaką organizacijos veiklos tęstinumui, reputacijai ir pacientų saugai.

Vienas ekspertas pažymėjo:

„Strateginiuose dokumentuose saugumas dažnai atsiranda kaip bendras punktas, bet jis netampa realiu sprendimų kriterijumi“ (E1, asmeninis interviu, 2024-07-08).

Ši įžvalga atskleidžia esminę problemą – strateginį planavimą dažnai apriboja deklaratyviais tikslais, kurie nėra susiejami su konkrečiais rodikliais, investicijomis ar atsakomybėmis. Kibernetinis saugumas tampa antrine tema, kuri konkuruoja su klinikiniais, finansiniais ar infrastruktūros prioritetais ir dažnai pralaimi šią konkurenciją.

Kitas ekspertas pabrėžė ilgalaikės vizijos trūkumą:

„Nėra aiškaus supratimo, kaip saugumas turėtų vystytis ilgalaikėje perspektyvoje. Sprendimai dažniausiai trumpalaikiai“ (E4, asmeninis interviu, 2024-07-15).

Tokia situacija lemia, kad saugumo iniciatyvos įgyvendinamos projektiniu principu, be tarpusavio suderinamumo ir tęstinumo. Ekspertų nuomone, tai ypač pavojinga e. sveikatos sistemose, kurios pasižymi dideliu technologiniu sudėtingumu ir tarpinstitucine priklausomybe.

Teminė analizė aiškiai parodė, kad vadovybės vaidmuo yra vienas kritinių veiksnių, lemiančių kibernetinio saugumo valdymo brandą. Ekspertai pabrėžė, jog vadovybės

požiūris formuoja ne tik sprendimų priėmimo kryptį, bet ir visos organizacijos saugumo kultūrą.

Vienas ekspertas teigė:

„Jeigu vadovybė nemato saugumo kaip savo atsakomybės, jis automatiškai tampa techniniu klausimu“ (E7, asmeninis interviu, 2024-07-22).

Tokiu atveju kibernetinis saugumas deleguojamas informacinių technologijų ar saugumo specialistams, kurie dažnai neturi pakankamų įgaliojimų inicijuoti strateginius pokyčius. Ekspertų nuomone, tai sukuria struktūrinį disbalansą, kai sprendimų priėmimo galia ir atsakomybė už rizikas nėra suderintos.

Kitas ekspertas pažymėjo reaktyvų vadovybės elgesį:

„Vadovybės dėmesys saugumui dažniausiai atsiranda po incidentų, o ne prieš juos“ (E9, asmeninis interviu, 2024-07-25).

Šis požiūris lemia, kad saugumas tampa „kriziniu klausimu“, o ne nuolatine valdymo funkcija. Ekspertų vertinimu, toks reagavimo modelis yra ypač pavojingas e. sveikatos sektoriuje, kur net trumpalaikiai sistemos sutrikimai gali turėti tiesioginį poveikį pacientų saugai.

Kita reikšminga teminė kategorija – organizacinės struktūros ir atsakomybių paskirstymas. Ekspertų interviu atskleidė, kad kibernetinio saugumo funkcijos sveikatos sektoriuje dažnai yra išskaidytos tarp kelių padalinių, o aiškaus atsakomybės centro nėra.

Vienas ekspertas situaciją apibūdino taip:

„Kai atsakomybė išskaidyta, realiai niekas nesijaučia galutinai atsakingas“ (E2, asmeninis interviu, 2024-07-09).

Ekspertai pabrėžė, kad atsakomybės dažnai persidengia tarp informacinių technologijų skyriaus, administracijos, išorinių tiekėjų ir institucijų. Tai ypač išryškėja incidentų metu, kai neaišku, kas turi inicijuoti sprendimus ir koordinuoti veiksmus.

Kitas ekspertas pažymėjo:

„Incidento metu paaiškėja, kad atsakomybės buvo aprašytos tik teoriškai“ (E8, asmeninis interviu, 2024-07-23).

Tokios organizacinės spragos mažina reagavimo greitį ir didina incidentų pasekmių mastą. Ekspertų nuomone, aiškiai apibrėžtos atsakomybės yra būtina sąlyga strateginiam kibernetinio saugumo valdymui.

Ekspertai daug dėmesio skyrė organizacinės saugumo kultūros klausimams. Jų nuomone, saugumo kultūra e. sveikatos sektoriuje dar tik formuojasi ir dažnai konkuruoja su klinikiniais prioritetais.

Vienas ekspertas teigė:

„Medicinos personalas pirmiausia orientuotas į pacientą, o saugumas dažnai suvokiamas kaip trukdis“ (E5, asmeninis interviu, 2024-07-16).

Kitas ekspertas papildė:

„Saugumo kultūra negali būti įdiegta vien mokymais. Ji turi būti organizacijos vertybių dalis“ (E7, asmeninis interviu, 2024-07-22).

Ekspertų nuomone, saugumo kultūros trūkumas lemia žmogiškojo faktoriaus dominavimą incidentų struktūroje. Net ir turint aiškias taisykles, jų laikymasis tampa

selektyvus, jei saugumas nėra suvokiamas kaip bendra organizacinė atsakomybė.

Teminė analizė atskleidė, kad strateginio ir organizacinio valdymo problematika ypač ryški tarpinstituciniame lygmenyje. E. sveikatos sistema veikia kaip kompleksinė ekosistema, kurioje pavienių organizacijų sprendimai turi poveikį visai sistemai.

Vienas ekspertas pažymėjo:

„Vienos įstaigos saugumo spraga gali turėti poveikį visai sistemai“ (E1, asmeninis interviu, 2024-07-08).

Ekspertai pabrėžė bendros strateginės krypties stoką:

„Kiekviena institucija sprendžia savaip, bet nėra vieningo strateginio rėmo“ (E9, asmeninis interviu, 2024-07-25).

Tai lemia kad, kai saugumo lygis visoje sistemoje tampa nenuoseklus, o silpniausia grandis kelia grėsmę visai ekosistemai.

Apibendrinant teminės ekspertinių interviu analizės rezultatus, galima teigti, kad strateginio ir organizacinio kibernetinio saugumo valdymo problematika e. sveikatos sistemoje yra fundamentali ir sisteminė. Ekspertų įžvalgos rodo, jog pagrindiniai iššūkiai kyla ne dėl technologijų stokos, bet dėl nepakankamos strateginės integracijos, riboto vadovybės įsitraukimo, fragmentuoto atsakomybių paskirstymo, silpnos saugumo kultūros ir neefektyvaus tarpinstitucinio koordinavimo.

Šios problemos lemia, kad kibernetinis saugumas dažnai vystomas reaktyviai ir epizodiškai, o ne kaip ilgalaikė, strateginė organizacijos ir visos e. sveikatos sistemos atsparumo funkcija. Identifikuotos teminės įžvalgos nukreipia kitame poskyryje pereiti prie technologinio saugumo ir procesų brandos vertinimo, papildant strateginio ir organizacinio lygmens analizę technologiniu ir operaciniu pjūviais.

3.2.2. Technologinio saugumo ir procesų brandos vertinimas

Šiame poskyryje pateikiama teminė ekspertinių interviu analizė, orientuota į technologinio kibernetinio saugumo lygio ir su juo susijusių organizacinių procesų brandos vertinimą e. sveikatos sistemoje. Skirtingai nei ankstesniame poskyryje nagrinėta strateginio ir organizacinio valdymo problematika, ši analizė leidžia detaliau atskleisti, kaip technologiniai sprendimai, saugumo procesai ir jų tarpusavio sąveika realiai veikia praktikoje bei kokią įtaką jie daro bendram sistemos atsparumui.

Ekspertų vertinimu, technologinis kibernetinis saugumas sveikatos sektoriuje dažnai suvokiamas kaip pagrindinis ir kartais net vienintelis saugumo elementas. Tačiau ekspertinės įžvalgos rodo, kad technologijų diegimas be procesinės ir organizacinės brandos sukuria tik tariamą saugumo pojūtį, kuris realių incidentų metu ne visada pasiteisina.

Vienas iš dažniausiai ekspertų pabrėžtų aspektų – itin nevienodas technologinio saugumo brandos lygis skirtingose sveikatos sektoriaus organizacijose. Ekspertai nurodė, kad didesnės organizacijos ar nacionalinio lygmens institucijos dažniau diegia pažangias saugumo technologijas, tuo tarpu mažesnės įstaigos apsiriboja minimaliais sprendimais.

Vienas ekspertas pažymėjo:

„Technologinis saugumas labai priklauso nuo organizacijos dydžio ir finansinių galimybių“ (E3, asmeninis interviu, 2024-07-11).

Kitas ekspertas papildė:

„Kai kur matome labai pažangias sistemas, bet kitur saugumas apsiriboja antivirusine programine įranga ir ugniasiene“ (E6, asmeninis interviu, 2024-07-18).

Toks nevienodumas lemia bendros e. sveikatos sistemos pažeidžiamumą, nes technologinis saugumas veikia kaip tarpusavyje susietų komponentų visuma. Ekspertų nuomone, silpniausia grandis tampa potencialiu įėjimo tašku kibernetinėms atakoms, nepriklausomai nuo kitų institucijų investicijų.

Teminė analizė atskleidė, kad viena esminių technologinio saugumo problemų yra fragmentiškas technologijų diegimas, nesant aiškios saugumo architektūros ir ilgalaikės vizijos.

Vienas ekspertas situaciją apibūdino taip:

„Technologijos dažnai diegiamos kaip pavieniai sprendimai, o ne kaip vientisa sistema“ (E5, asmeninis interviu, 2024-07-16).

Kitas ekspertas pabrėžė:

„Trūksta bendro architektūrinio požiūrio – kiekvienas projektas sprendžia savo problemą“ (E1, asmeninis interviu, 2024-07-08).

Ekspertų vertinimu, toks požiūris lemia saugumo sprendimų dubliavimą, sudėtingą priežiūrą ir ribotą tarpusavio integraciją. Technologijos tampa sunkiai valdomos, o saugumo incidentų metu informacija apie įvykius nėra konsoliduojama vieningoje sistemoje.

Technologinio saugumo brandą ekspertai glaudžiai siejo su stebėsenos, incidentų aptikimo ir reagavimo procesų išvystymu. Nors tam tikros techninės priemonės dažnai egzistuoja, jų praktinis panaudojimas ir procesinis integravimas vertinamas kritiškai.

Vienas ekspertas teigė:

„Stebėsenos įrankiai yra, bet ne visada aišku, kas ir kaip į juos reaguoja“ (E8, asmeninis interviu, 2024-07-23).

Kitas ekspertas papildė:

„Technologijos fiksuoja įvykius, bet trūksta aiškaus reagavimo proceso“ (E7, asmeninis interviu, 2024-07-22).

Tai rodo, kad technologinis saugumas dažnai apsiriboja duomenų rinkimu, tačiau nesukuria realios pridėtinės vertės be aiškiai apibrėžtų procesų ir atsakomybės.

Ekspertai pabrėžė, kad daugelyje organizacijų saugumo procesai egzistuoja dokumentiniu lygmeniu, tačiau jų praktinis įgyvendinimas yra ribotas.

Vienas ekspertas pažymėjo:

„Procedūros aprašytos, bet realiai jomis vadovaujamasi tik iš dalies“ (E2, asmeninis interviu, 2024-07-09).

Kitas ekspertas akcentavo atotrūkį tarp teorijos ir praktikos:

„Dokumentai neatspindi realaus darbo tempo ir įvykstančių situacijų“ (E4, asmeninis interviu, 2024-07-15).

Ekspertų nuomone, procesų formalizavimas be nuolatinio testavimo, atnaujinimo ir darbuotojų įtraukimo nesukuria brandžios saugumo sistemos.

Ypatingas dėmesys ekspertų interviu metu buvo skirtas medicininėms informacinėms sistemoms, kurios pasižymi specifiniais saugumo reikalavimais.

Vienas ekspertas pažymėjo:

„Medicininės sistemos dažnai yra senos, bet labai svarbios, todėl jų keitimas sudėtingas“ (E6, asmeninis interviu, 2024-07-18).

Kitas ekspertas papildė:

„Negalima tiesiog išjungti sistemos dėl atnaujinimo – tai riboja saugumo priemonių diegimą“ (E3, asmeninis interviu, 2024-07-11).

Tai rodo, kad technologinio saugumo sprendimai turi būti derinami su klinikiniais procesais, o standartiniai informacinių technologijų saugumo modeliai ne visada tinkami be adaptacijos.

Ekspertai pabrėžė, kad technologinio saugumo procesai dažnai nėra grindžiami nuolatinio tobulinimo logika.

Vienas ekspertas teigė:

„Po incidento dažnai grįžtama prie įprastos veiklos, neanalizuojant priežasčių“ (E5, asmeninis interviu, 2024-07-16).

Kitas ekspertas pridūrė:

„Nėra aiškaus ciklo – planuoti, įgyvendinti, tikrinti, tobulinti“ (E9, asmeninis interviu, 2024-07-25).

Tai rodo, kad procesų brandos lygis dažnai apsiriboja baziniu reagavimo etapu ir nepasiekia aukštesnių brandos lygių, kuriuose saugumas tampa nuolat tobulinama sistema.

Ekspertai akcentavo, kad technologinis saugumas negali būti vertinamas atskirai nuo darbuotojų kompetencijos.

Vienas ekspertas pažymėjo:

„Technologijos be darbuotojų kompetencijų neveikia“ (E7, asmeninis interviu, 2024-07-22).

Kitas ekspertas papildė:

„Dažnai turime įrankius, bet neturime žmonių, kurie galėtų juos maksimaliai išnaudoti“ (E1, asmeninis interviu, 2024-07-08).

Tai rodo, kad technologinio saugumo brandai būtinas nuoseklus darbuotojų kompetencijų ugdymas ir jų įtraukimas į saugumo procesus.

Apibendrinant teminės ekspertinių interviu analizės rezultatus, galima teigti, kad technologinio saugumo ir procesų brandos lygis e. sveikatos sistemoje yra nevienalytis, fragmentuotas ir dažnai nepakankamai integruotas. Nors egzistuoja atskiri pažangūs technologiniai sprendimai, jų efektyvumą riboja procesų nebrandumas, nepakankama integracija, riboti žmogiškieji ištekliai ir nuolatinio tobulinimo stokos.

Ekspertų įžvalgos patvirtina, kad technologinis saugumas turi būti integruotas į platesnę strateginio ir organizacinio valdymo sistemą. Šios išvados sudaro empirinį pagrindą kitame poskyryje pereiti prie teisinio reglamentavimo ir praktinio įgyvendinimo atotrūkių analizės, leidžiančios papildyti technologinį vertinimą reguliaciniu ir institucinės atitikties pjūviu.

3.2.3. Teisinio reglamentavimo ir praktinio įgyvendinimo atotrūkiai

Teisinis kibernetinio saugumo reglamentavimas e. sveikatos sistemoje sudaro formaliąją saugumo valdymo ašį, apibrėžiančią privalomus reikalavimus, atsakomybes ir kontrolės mechanizmus. Tačiau vien teisės aktų egzistavimas savaime neužtikrina nei veiksmingo kibernetinio saugumo, nei realaus organizacijų atsparumo kibernetinėms grėsmėms. Ekspertinių interviu analizė atskleidė ryškų ir sisteminį atotrūkį tarp formalaus teisinio reglamentavimo ir jo praktinio įgyvendinimo sveikatos sektoriuje. Šis atotrūkis pasireiškia tiek strateginiame, tiek operaciniame lygmenyje ir yra vienas iš pagrindinių veiksnių, ribojančių kibernetinio saugumo valdymo brandą e. sveikatos sistemoje.

Ekspertų nuomone, sveikatos sektorius veikia itin sudėtingoje reguliacinėje aplinkoje, kurioje persipina nacionaliniai teisės aktai, Europos Sąjungos reglamentai, sektoriniai reikalavimai ir bendrieji informacijos saugumo standartai. Tačiau ši reguliacinė gausa ne visada transformuojasi į aiškų, organizacijoms suprantamą ir praktiškai įgyvendinamą saugumo valdymo modelį. Kaip pažymėjo vienas ekspertas:

„Teisės aktų turime daug, bet jie tarpusavyje ne visada suderinti. Organizacijos dažnai nežino, kuris reikalavimas yra svarbesnis, o kuris tik deklaratyvus“ (E1, asmeninis interviu, 2024-07-08).

Ši įžvalga atskleidžia vieną esminių problemų – normatyvinio reguliavimo fragmentiškumą. Ekspertai pabrėžė, kad kibernetinio saugumo reikalavimai sveikatos sektoriuje dažnai atsiranda kaip reakcija į išorinius politinius ar reguliacinius impulsus (pvz., naujas ES direktyvas), tačiau nėra pakankamai integruojami į esamą nacionalinę ir sektorinę reguliavimo architektūrą. Dėl to organizacijos susiduria su situacija, kai reikalavimai formaliai egzistuoja, bet jų praktinė reikšmė ir tarpusavio ryšiai lieka neaiškūs.

Ypač ryškus ekspertų akcentuotas aspektas – teisinio reguliavimo abstraktumas. Nors teisės aktuose dažnai įtvirtinami bendrieji kibernetinio saugumo principai, jie retai pateikia konkrečias gaires, kaip šie principai turėtų būti įgyvendinami praktikoje, atsižvelgiant į sveikatos sektoriaus specifiką. Vienas ekspertas šią problemą apibūdino taip:

„Teisės aktai sako, kad turi būti „užtikrintas saugumas“, bet nepasako, kaip tai padaryti ligoninėje, kur prioritetas yra pacientas, o ne IT“ (E6, asmeninis interviu, 2024-07-18).

Ši citata atskleidžia struktūrinį neatitikimą tarp normatyvinio saugumo diskurso ir realios sveikatos įstaigų veiklos logikos. Ekspertų teigimu, teisiniai reikalavimai dažnai kuriami remiantis universaliu informacijos saugumo modeliu, kuris nepakankamai atsižvelgia į klinikinių procesų nenutrūkstamumą, medicininių technologijų specifiką ir kritinį laiko faktorių. Dėl to praktikoje organizacijos priverstos improvizuoti, bandydamos suderinti formalią atitiktį su kasdieniais veiklos poreikiais.

Ekspertai taip pat pabrėžė, kad teisinis reguliavimas dažnai suvokiamas kaip atitikties našta, o ne kaip priemonė stiprinti organizacijos atsparumą. Šis požiūris ypač ryškus mažesnėse sveikatos įstaigose, kuriose trūksta specializuotų teisininkų ir

kibernetinio saugumo specialistų. Kaip pažymėjo vienas ekspertas:

„Daugelyje įstaigų saugumas daromas tam, kad nebūtų baudos, o ne tam, kad sistema būtų saugesnė“ (E4, asmeninis interviu, 2024-07-15).

Tokio pobūdžio atitikties orientacija lemia paviršutinišką teisinio reguliavimo įgyvendinimą, dokumentai rengiami formaliai, procedūros dokumentuojamos, tačiau realūs procesai lieka nepakitę. Ekspertai pabrėžė, kad tokia praktika ypač pavojinga e. sveikatos kontekste, nes klaidina ir didina sisteminių incidentų riziką.

Kitas svarbus ekspertų identifikuotas atotrūkio aspektas – institucinis neapibrėžtumas. Nors teisės aktuose dažnai nurodomos bendros atsakomybės, praktikoje lieka neaišku, kuri institucija yra atsakinga už koordinuotą kibernetinio saugumo valdymą e. sveikatos sistemos mastu. Vienas ekspertas šią problemą apibūdino taip:

„Reglamentavimas išskaidytas tarp skirtingų institucijų, bet realaus koordinavimo trūksta“ (E9, asmeninis interviu, 2024-07-25).

Ekspertų nuomone, toks fragmentuotas reguliacinis valdymas lemia tai, kad sveikatos įstaigos gauna skirtingus, kartais net prieštaringus signalus iš skirtingų priežiūros institucijų. Tai apsunkina nuoseklaus kibernetinio saugumo valdymo diegimą ir skatina minimalios atitikties strategijas.

Reikšminga ekspertų įžvalgų dalis buvo susijusi su TIS2 direktyvos ir kitų naujų ES kibernetinio saugumo reikalavimų įgyvendinimu. Nors ekspertai pripažino šių iniciatyvų svarbą, jie taip pat pabrėžė, kad praktinis pasirengimas joms sveikatos sektoriuje yra ribotas. Vienas ekspertas teigė:

„Reikalavimai ateina greičiau nei gebėjimas juos įgyvendinti“ (E2, asmeninis interviu, 2024-07-09).

Ši situacija ypač aktuali e. sveikatos sistemoje, kuri pasižymi sudėtingomis integracijomis ir ribotais finansiniais bei žmogiškaisiais ištekliais. Ekspertai pabrėžė, kad be papildomų metodinių gairių, kompetencijų stiprinimo ir centralizuotos pagalbos nauji teisiniai reikalavimai gali dar labiau padidinti atotrūkį tarp normos ir praktikos.

Ekspertų interviu taip pat atskleidė problemą, susijusią su teisinio reglamentavimo ir technologinės realybės neatitikimu. Daugelis teisės aktų, ekspertų nuomone, nepakankamai atsižvelgia į medicininių įrenginių, paveldėtų informacinių sistemų ir tarp organizacinių integracijų saugumo ypatumus. Kaip pažymėjo vienas ekspertas:

„Teisės aktai dažnai orientuoti į klasikines IT sistemas, bet ne į realią e. sveikatos infrastruktūrą“ (E5, asmeninis interviu, 2024-07-16).

Šis neatitikimas lemia, kad organizacijos priverstos rinktis kompromisinius sprendimus, kurie formaliai atitinka reguliavimą, bet ne visada užtikrina realų saugumą. Ekspertai pabrėžė, kad tokia situacija ilgainiui silpnina pasitikėjimą pačiu teisiniu reglamentavimu kaip efektyvia valdymo priemone.

Apibendrinant ekspertų interviu analizę, galima teigti, kad teisinio reglamentavimo ir praktinio įgyvendinimo atotrūkiai e. sveikatos sistemoje yra sisteminiai, daugiasluoksniai ir glaudžiai susiję su strateginio valdymo, institucinės koordinacijos, organizacinių kompetencijų ir technologinės brandos problemomis. Šie atotrūkiai lemia, kad kibernetinio saugumo valdymas dažnai tampa formaliu atitikties procesu, o ne integruota, į atsparumą orientuota sistema.

Ekspertų įžvalgos patvirtina, kad vienas esminių iššūkių nėra naujų teisės aktų trūkumas, bet gebėjimas juos prasmingai įgyvendinti e. sveikatos kontekste. Todėl siūlomo kibernetinio saugumo valdymo modelio tikslinimas turi būti orientuotas ne tik į normatyvinės bazės atitikimą, bet ir į praktinius mechanizmus, leidžiančius sumažinti atotrūkį tarp teisinio reguliavimo ir realios organizacijų veiklos.

Ši teminė analizė sudaro svarbų empirinį pagrindą kitame skyriuje pereiti prie modelio tikslinimo remiantis ekspertinio tyrimo rezultatais, kur bus sistemiškai integruojamos identifikuotos problemos ir formuluojami struktūriniai bei funkciniai sprendimai, skirti kibernetinio saugumo valdymo brandai stiprinti e. sveikatos sistemoje.

3.3. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui tikslinimas remiantis ekspertinio tyrimo rezultatais

Šiame disertacijos skyriuje pateikiamas sukurto kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui adaptavimas ir tikslinimas, remiantis empirinio ekspertinio tyrimo rezultatais. Skirtingai nei ankstesniuose skyriuose, kuriuose buvo analizuojama esama kibernetinio saugumo būklė, identifikuojamos spragos ir vertinamos valdymo praktikos, šiame skyriuje pereinama nuo diagnostinės analizės prie konstruktyvaus sprendimo formavimo.

Modelio tikslinimas grindžiamas nuostata, kad efektyvus kibernetinio saugumo valdymas e. sveikatos sistemoje negali būti kuriamas vien teoriniu ar normatyviniu pagrindu. Atsižvelgiant į e. sveikatos sistemų pobūdį, būtina integruoti realias organizacines, institucinės sąveikos, technologines ir žmogiškąsias praktikas, kurios buvo atskleistos ekspertų interviu metu. Todėl ekspertinio tyrimo rezultatai šiame skyriuje traktuojami ne kaip papildoma iliustracinė medžiaga, bet kaip esminis modelio adaptavimo ir validavimo šaltinis.

Ekspertų pateiktos įžvalgos leido identifikuoti ne tik pavienes kibernetinio saugumo problemas, bet ir jų tarpusavio sąsajas, struktūrinius pasikartojimus bei sistemines priežastis. Tyrimo metu išryškėjo, kad daugelis kibernetinio saugumo spragų e. sveikatos sistemoje kyla ne dėl techninių priemonių stokos, o dėl nepakankamai aiškaus valdymo modelio, fragmentuoto atsakomybės paskirstymo, ribotos strateginės lyderystės ir silpnos grįžtamojo ryšio integracijos į sprendimų priėmimo procesus. Šių įžvalgų empiriniu pagrindu buvo peržiūrėtas ir patikslintas pradiniame disertacijos etape suformuotas kibernetinio saugumo valdymo modelis.

Modelio tikslinimas buvo vykdomas laikantis dizaino mokslo tyrimų (*angl. Design Science Researc*h) metodologijos principų, kuriuose akcentuojamas modelio kūrimas, vertinimas ir tobulinimas remiantis empiriniais duomenimis. Šiame kontekste ekspertinis vertinimas atliko dvigubą funkciją. Pirma, leido identifikuoti kritines kibernetinio saugumo valdymo sritis, kurioms būtina struktūrinė intervencija, ir, antra, suteikė galimybę patikrinti, ar siūlomas modelis atitinka realius e. sveikatos sistemos veikimo poreikius.

Remiantis teminės ekspertinių interviu analizės rezultatais, modelio tikslinimas buvo orientuotas į šias pagrindines kryptis:

1. strateginio ir organizacinio kibernetinio saugumo valdymo stiprinimą,
2. aiškesnį valdymo lygių ir atsakomybių diferencijavimą,
3. rizikų ir incidentų valdymo integravimą į nuolatinio tobulinimo ciklą,
4. technologinių sprendimų derinimą su organizaciniais procesais,
5. tarpinstitucinio koordinavimo ir informacijos srautų valdymo stiprinimą.

Svarbu pabrėžti, kad modelio tikslinimas nebuvo vykdomas kaip visiškai naujos koncepcijos kūrimas, o kaip pradinio modelio struktūrinė ir funkcinė adaptacija, siekiant padidinti jo praktinį taikymą e. sveikatos sistemos kontekste. Tokiu būdu išlaikomas teorinis nuoseklumas su pirmuose disertacijos skyriuose analizuotais kibernetinio saugumo valdymo modeliais, kartu integruojant empiriškai pagrįstas ekspertų įžvalgas.

Atsižvelgiant į tai, šiame skyriuje modelio tikslinimas pristatomas trimis nuosekliais etapais. Pirmiausia identifikuojamos kritinės kibernetinio saugumo valdymo sritys, kurioms būtina intervencija (3.3.1 poskyris). Antrajame etape pateikiami konkretūs struktūriniai ir funkciniai siūlymai, integruojami į siūlomą valdymo modelį (3.3.2 poskyris). Galiausiai aptariamas patikslinto modelio adaptavimas praktiniam taikymui e. sveikatos sistemoje, įvertinant jo lankstumą, taikymo sąlygas ir galimus ribotumus (3.3.3 poskyris).

Tokiu būdu 3.3 skyrius sujungia empirinę analizę ir baigiamąsias disertacijos išvadas, atskleisdamas, kaip ekspertinio tyrimo rezultatai transformuojami į moksliškai pagrįstą ir praktiškai pritaikomą kibernetinio saugumo valdymo modelį e. sveikatos sistemos tobulinimui.

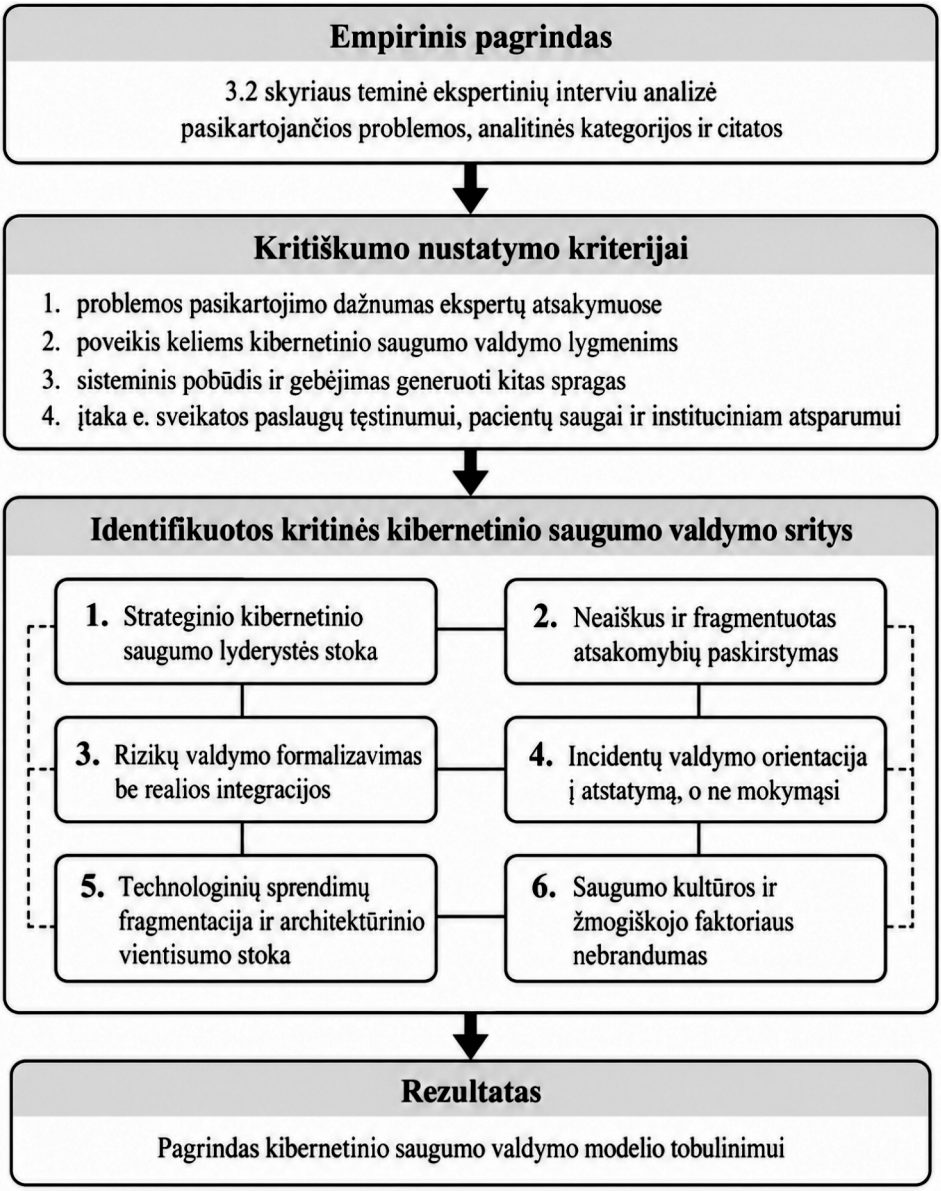
3.3.1. Kritinių kibernetinio saugumo valdymo sričių identifikavimas

Kritinių kibernetinio saugumo valdymo sričių identifikavimas yra esminis etapas tobulinant siūlomą kibernetinio saugumo valdymo modelį e. sveikatos sistemos kontekste. Šiame poskyryje siekiama sistemiškai apibendrinti ekspertinio tyrimo metu išryškėjusias problemas ir transformuoti jas į aiškiai apibrėžtas valdymo sritis, kurioms būtina struktūrinė, organizacinė ar funkcinė intervencija. Tokia prieiga leidžia pereiti nuo ekspertinių įžvalgų analizės prie normatyvinio modelio tikslinimo.

Kritinės sritys identifikuojamos remiantis 3.2 skyriuje atlikta temine ekspertinių interviu analize, kurioje ekspertų atsakymai buvo sugrupuoti pagal pasikartojančias problemas, analitines kategorijas ir jas pagrindžiančias citatas. Ši analizė atlieka konceptualaus „tilto“ funkciją tarp empirinių duomenų ir modelio konstravimo, leidžiančio užtikrinti, kad siūlomi sprendimai būtų empiriškai pagrįsti, o ne deklaratyvūs.

Analizuojant interviu metu išskirtas problemas, buvo taikomi šie kriterijai kritiškumui nustatyti: problemos pasikartojimo dažnumas skirtingų ekspertų atsakymuose; problemos poveikis keliems kibernetinio saugumo valdymo lygiams (strateginiam, organizaciniam, operaciniam, technologiniam); problemos sisteminis pobūdis, t. y. jos gebėjimas generuoti kitas spragas; tiesioginė ar netiesioginė įtaka e. sveikatos paslaugų tęstinumui, pacientų saugai ir instituciniam atsparumui.

Remiantis šiais kriterijais, identifikuotos šešios tarpusavyje susijusios kritinės kibernetinio saugumo valdymo sritys, kurios detalizuojamos 8 pav.



8 pav. Problemos, išryškėjusios ekspertų interviu metu.

Šaltinis: sudaryta autorės

Viena ryškiausių ir sisteminių problemų (žr. 8 pav.), išryškėjusių ekspertų interviu metu, yra strateginio kibernetinio saugumo lyderystės stoka sveikatos sektoriaus

organizacijose. Beveik visi ekspertai tiesiogiai arba netiesiogiai akcentavo, kad kibernetinis saugumas dažnai nėra suvokiamas kaip strateginis organizacijos valdymo elementas. Ekspertų įžvalgos rodo, kad saugumas dažniausiai deleguojamas techniniam lygmeniui, paliekant jį informacinių technologijų skyriui ar informacijos saugumo specialistų atsakomybei, o vadovybės vaidmuo apsiriboja formaliu dokumentų tvirtinimu. Dėl to kibernetinis saugumas nėra integruojamas į strateginius sprendimus, investicijų planavimą ar organizacinių pokyčių valdymą. Ši problema laikytina kritine, todėl strateginės lyderystės stiprinimas tampa būtina sąlyga bet kokiam modelio tikslinimui.

Antroji kritinė sritis yra neaiškus ir fragmentuotas atsakomybių paskirstymas kibernetinio saugumo valdymo srityje. Ekspertai pabrėžė, kad daugelyje sveikatos įstaigų nėra aiškiai apibrėžta, kas atsakingas už saugumą strateginiu, taktiniu ir operaciniu lygmenimis. Ši problema ypač ryški e. sveikatos ekosistemoje, kurioje dalyvauja kelios institucijos ar išoriniai tiekėjai. Tokiomis sąlygomis atsakomybės išskaidymas be aiškaus koordinavimo mechanizmo lemia sprendimų vilkinimą, konfliktines situacijas incidentų metu ir sumažėjusį reagavimo efektyvumą. Ekspertų atsakymai leidžia teigti, kad atsakomybių neapibrėžtumas tampa struktūrine kliūtimi įgyvendinti brandų kibernetinio saugumo valdymo modelį. Todėl ši sritis identifikuojama kaip viena iš pagrindinių modelio tikslinimo krypčių.

Trečioji kritinė sritis susijusi su rizikų valdymo praktikos nebrandumu. Ekspertai vieningai pažymėjo, kad rizikų vertinimas dažnai egzistuoja kaip formali, reglamentų nulemta procedūra, tačiau nėra integruotas į realų sprendimų priėmimą. Rizikų analizės rezultatai retai daro įtaką biudžeto planavimui, technologinių sprendimų pasirinkimui ar organizacinių prioritetų nustatymui. Dėl to rizikų valdymas tampa atskirta funkcija, neturinčia realios galios formuoti saugumo politiką. Ši spraga laikytina kritine, nes rizikų valdymas yra centrinė jungtis tarp grėsmių identifikavimo ir valdymo sprendimų. Be jos neįmanoma pereiti nuo reaktyvaus prie proaktyvaus kibernetinio saugumo modelio.

Ketvirtoji kritinė sritis susijusi su incidentų valdymo praktika. Ekspertų atsakymai rodo, kad daugelyje sveikatos įstaigų incidentų valdymas orientuotas į operatyvų paslaugų atstatymą, tačiau stokojama sisteminio mokymosi po incidentų. Incidentų analizė dažnai apsiriboja techninių priežasčių nustatymu, neįvertinant organizacinių, procesinių ar žmogiškųjų veiksnių. Ekspertų nuomone, tai rodo ne tik procedūrų trūkumą, bet ir organizacinės kultūros problemą, kurioje saugumo incidentai suvokiami kaip nepageidautini įvykiai, o ne kaip tobulinimosi šaltinis.

Penktąją kritinę sritį sudaro technologinių sprendimų fragmentacija. Nors ekspertai pripažįsta, kad technologinių saugumo priemonių spektras sveikatos sektoriuje plečiasi, jų diegimas dažnai vyksta be bendros architektūrinės vizijos. Tai lemia saugumo priemonių dubliavimą, nesuderinamumą ir ribotas duomenų mainų galimybes. Ekspertų teigimu, technologinis saugumas dažnai neužtikrina sisteminio atsparumo. Ši problema laikytina kritine, nes technologiniai sprendimai be organizacinės integracijos ne tik nedidina saugumo, bet kartais net sukuria papildomas problemas.

Paskutinė, tačiau ne mažiau svarbi kritinė sritis – saugumo kultūros stoka. Kaip rodo 15 lentelėje pateiktos citatos, ekspertai vieningai pabrėžė, kad žmogiškasis

faktorius išlieka silpniausia kibernetinio saugumo grandimi. Darbuotojų sąmoningumas, mokymų kokybė ir požiūris į saugumą dažnai neatitinka realių grėsmių lygio. Tai ypač aktualu e. sveikatos kontekste, kur prioritetas teikiamas klinikiniams procesams, o saugumas suvokiamas kaip papildoma našta. Ši sritis laikytina kritine, nes be kultūrinės transformacijos net ir geriausi techniniai bei organizaciniai sprendimai nepasieks norimo efekto.

Apibendrinant galima teigti, kad 15 lentelėje išskirtos problemos leidžia identifikuoti šešias tarpusavyje susijusias kritines kibernetinio saugumo valdymo sritis. Šios sritys ne tik atspindi esamą kibernetinio saugumo nebrandumą e. sveikatos sistemoje, bet ir aiškiai nurodo, kuriose vietose intervencija turėtų būti struktūriškai integruota.

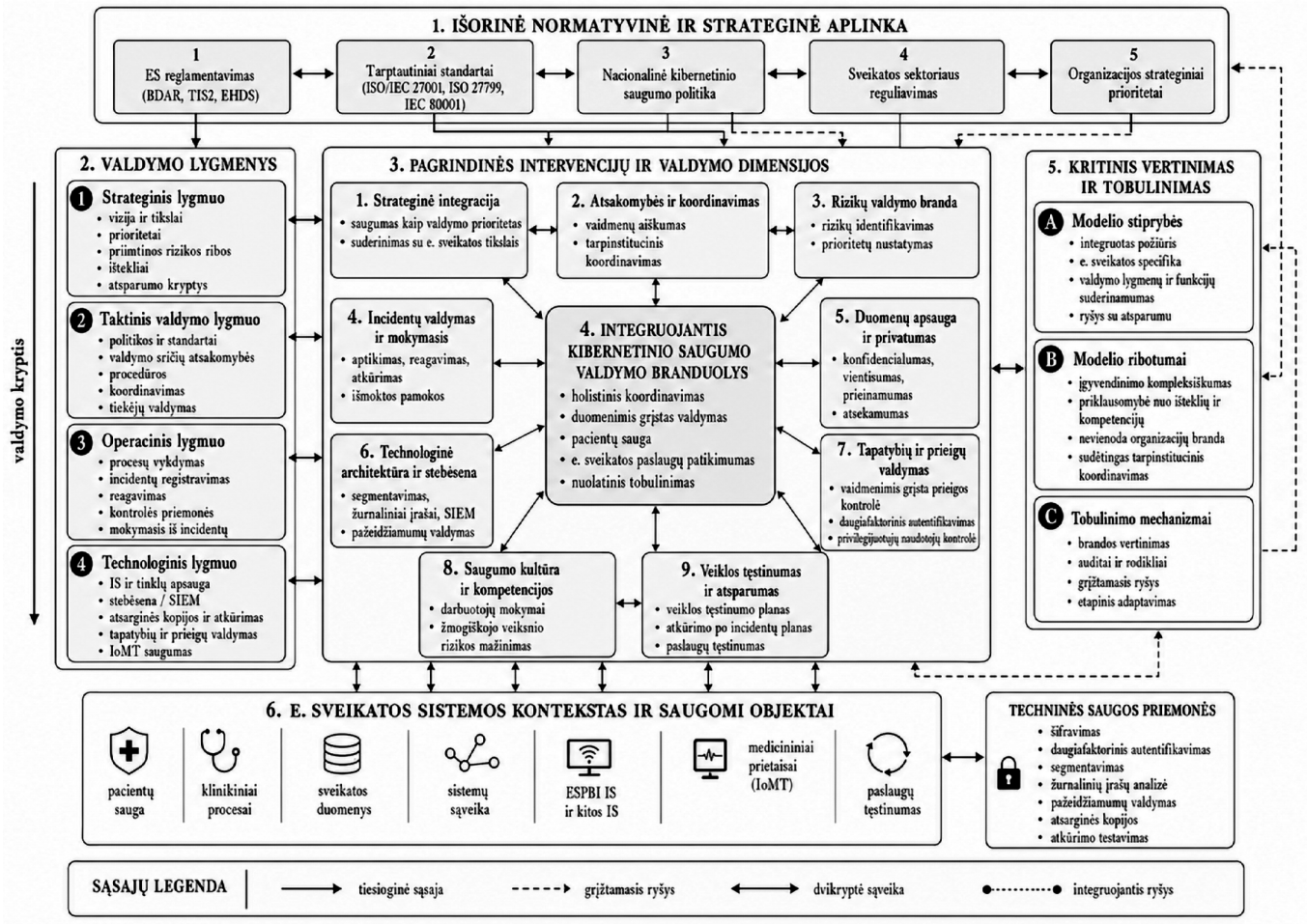
3.3.2. Patikslintas kibernetinio saugumo valdymo modelis e. sveikatos sistemos tobulinimui: struktūrinių ir funkcinių siūlymų integracija

Remiantis 3.3.1 poskyryje identifikuotomis kritinėmis kibernetinio saugumo valdymo sritimis ir 3.2 skyriuje atliktos ekspertinių interviu teminės analizės rezultatais, šiame poskyryje pereinama nuo problemų identifikavimo prie struktūrinių ir funkcinių sprendinių integravimo į patikslintą kibernetinio saugumo valdymo modelį e. sveikatos sistemos tobulinimui. Šis etapas žymi konceptualų perėjimą nuo teorinio ir empirinio problemos pagrindimo prie sistemingo valdymo sprendimo konstravimo, kuris atitinka dizaino mokslo tyrimų logiką, kai tyrimo rezultatas pateikiamas kaip praktiškai pritaikomas, teoriškai pagrįstas ir empiriškai tikslinamas artefaktas (Hevner ir kt., 2004; Peffers ir kt., 2007).

Ekspertinio tyrimo rezultatai atskleidė, kad pagrindinės e. sveikatos kibernetinio saugumo valdymo problemos nėra pavienės ar atsitiktinės. Jos formuoja tarpusavyje susijusią nepakankamai brandžios valdymo sistemos struktūrą, kurioje strateginio prioriteto stoka, neaiškios atsakomybės, fragmentiškas rizikų valdymas, ribotas incidentų analizavimas, technologinių sprendimų nesuderinamumas, tapatybių ir prieigų valdymo spragos bei saugumo kultūros trūkumas veikia kaip vienas kitą stiprinantys veiksniai. Dėl šios priežasties modelio tikslinimas negali būti fragmentiškas ar orientuotas tik į pavienių priemonių diegimą. Priešingai, būtina integruota struktūrinė ir funkcinė transformacija, apimanti strateginį, taktinį, operacinį ir technologinį valdymo lygmenis.

Patikslintas modelis formuojamas laikantis nuostatos, kad e. sveikatos kibernetinis saugumas turi būti suprantamas kaip socio-techninė valdymo sistema. Tai reiškia, kad technologinės priemonės, tokios kaip šifravimas, prieigos kontrolė, tinklų segmentavimas ar incidentų stebėsena, yra būtinos, tačiau nepakankamos, jeigu jos nėra susietos su organizacine atsakomybe, strateginiais prioritetais, rizikų vertinimu, darbuotojų kompetencijomis, teisiniu reguliavimu ir klinikinių paslaugų tęstinumo poreikiais. Toks požiūris atitinka mokslinėje literatūroje akcentuojamą kibernetinio saugumo kaip valdymo, o ne tik technologinės apsaugos reiškinio sampratą (Ransbotham ir kt., 2012; von Solms ir van Niekerk, 2018).

Patikslintas kibernetinio saugumo valdymo modelis e. sveikatos sistemos tobulinimui pateikiamas 9 paveiksle.



9 pav. Patikslintas kibernetinio saugumo valdymo modelis e. sveikatos sistemos tobulinimui.

Šaltinis: sudaryta autorės

9 paveiksle pateiktas patikslintas kibernetinio saugumo valdymo modelis e. sveikatos sistemos tobulinimui sudarytas iš šešių tarpusavyje susijusių struktūrinių dalių: išorinės normatyvinės ir strateginės aplinkos, valdymo lygmenų, pagrindinių intervencijų ir valdymo dimensijų, integruojančio kibernetinio saugumo valdymo branduolio, kritinio vertinimo ir tobulinimo bloko bei e. sveikatos sistemos konteksto ir saugomų objektų. Modelyje papildomai išskiriama techninių saugos priemonių sritis, kuri nėra savarankiškas modelio tikslas, bet palaiko bendrą kibernetinio saugumo valdymo sistemą technologinėmis kontrolės priemonėmis.

Tokia modelio struktūra pasirinkta siekiant parodyti, kad e. sveikatos sistemos kibernetinis saugumas negali būti grindžiamas vien techninių priemonių diegimu. Modelis jungia normatyvinius reikalavimus, organizacinius sprendimus, valdymo lygmenis, rizikų ir incidentų valdymo procesus, duomenų apsaugą, tapatybių ir prieigų valdymą, saugumo kultūrą, veiklos tęstinumą ir nuolatinį tobulinimą. Tokiu būdu modelis veikia kaip integruota vadybinė struktūra, leidžianti sistemiškai vertinti ir tobulinti kibernetinio saugumo valdymą e. sveikatos sistemos kontekste.

Modelio skaitymo logika grindžiama keliomis kryptimis. Pirmiausia, išorinė normatyvinė ir strateginė aplinka veikia kaip bendrasis modelio kontekstas, nustatantis teisinius, reguliacinius ir strateginius reikalavimus. Antra, valdymo lygmenys parodo, kaip kibernetinio saugumo sprendimai turi būti išdėstomi nuo strateginio sprendimo iki technologinio įgyvendinimo. Trečia, intervencijų ir valdymo dimensijos parodo, kokiose srityse turi vykti realus modelio stiprinimas. Ketvirta, integruojantis branduolys jungia atskiras dimensijas į vientisą valdymo sistemą. Penkta, kritinio vertinimo ir tobulinimo blokas leidžia modelį vertinti ne kaip galutinę schemą, bet kaip tobulinamą valdymo karkasą. Šešta, e. sveikatos sistemos kontekstas ir saugomi objektai parodo, kad modelis yra orientuotas ne į abstrakčią organizaciją, bet į konkrečią, aukštos rizikos, duomenimis ir paslaugų tęstinumu grįstą e. sveikatos ekosistemą.

Pirmoji modelio zona – išorinė normatyvinė ir strateginė aplinka – apima Europos Sąjungos reguliavimą, tarptautinius standartus, nacionalinę kibernetinio saugumo politiką, sveikatos sektoriaus reguliavimą ir organizacijos strateginius prioritetus. Šios zonos įtraukimas į modelį svarbus todėl, kad e. sveikatos kibernetinio saugumo valdymas negali būti suprantamas tik kaip vidinis organizacijos IT procesas. E. sveikatos sistemoje tvarkomi jautrūs asmens sveikatos duomenys, veikia tarpinstitucinės duomenų mainų sąsajos, naudojamos nacionalinės informacinės sistemos ir teikiamos paslaugos, kurių sutrikimas gali turėti tiesioginį poveikį pacientų saugai. Todėl kibernetinio saugumo valdymas turi būti derinamas su BDAR, TIS2, EHDS, ISO/IEC 27001, ISO/IEC 27799, IEC 80001 ir kitais sveikatos sektoriui aktualiais reikalavimais.

Išorinės aplinkos įtraukimas taip pat leidžia išvengti klaidingos prielaidos, kad kibernetinio saugumo valdymo modelis gali būti taikomas izoliuotai nuo reguliacinių reikalavimų. Ekspertinio tyrimo rezultatai parodė, kad organizacijos dažnai suvokia reguliacinius reikalavimus kaip formalią prievolę, tačiau ne visada integruoja juos į kasdienius rizikų, incidentų, prieigų ir duomenų apsaugos procesus. Todėl modelyje išorinė normatyvinė aplinka susiejama ne tik su atitikties dokumentais, bet ir su strateginiais prioritetais, vadovybės atsakomybe, auditu ir nuolatiniu tobulinimu.

Antroji modelio zona – valdymo lygmenys – apima strateginį, taktinį, operacinį ir technologinį lygmenis. Strateginis lygmuo modelyje siejamas su vizija ir tikslais, prioritetais, rizikomis, ištekliais ir atsparumo kryptimis. Šis lygmuo yra aukščiausias valdymo sluoksnis, formuojantis organizacijos požiūrį į kibernetinį saugumą kaip ilgalaikę strateginę vertę. Mokslinėje literatūroje pabrėžiama, kad kibernetinis saugumas šiuolaikinėse organizacijose turi būti vertinamas kaip strateginis valdymo klausimas, susijęs su organizacijos paslaugų tęstinumu ir reputacija (Ransbotham ir kt., 2012; von Solms ir kt. 2004).

Ekspertų interviu atskleidė, kad būtent strateginiame lygmenyje dažnai pasireiškia sisteminės kibernetinio saugumo valdymo spragos. Ekspertai pabrėžė, kad daugelyje sveikatos sektoriaus organizacijų kibernetinis saugumas nėra pakankamai integruotas į bendrą organizacijos strategiją ir dažnai egzistuoja kaip atskiras dokumentas ar formalus reikalavimas, neturintis realios įtakos sprendimų priėmimui. Tokia situacija lemia, kad saugumo klausimai tampa antraeiliais, ypač konkuruojant su klinikiniais, finansiniais ar veiklos efektyvumo tikslais. Todėl patikslintame modelyje strateginis lygmuo sąmoningai išskiriamas kaip kryptį nustatantis ir kitus lygmenis integruojantis elementas.

Strateginiame lygmenyje taip pat svarbus kibernetinio saugumo kaip investicijos, o ne vien sąnaudų, suvokimas. Mokslinėje literatūroje pabrėžiama, kad organizacijos, kurios saugumą vertina tik kaip kaštų centrą, dažniausiai investuoja minimaliai ir reaguoja tik po incidentų, o organizacijos, kurios saugumą traktuoja kaip strateginę investiciją, siekia ilgalaikio atsparumo ir sisteminio brandos augimo (Gordon ir kt., 2011). Ekspertinio tyrimo duomenys patvirtino, kad e. sveikatos sektoriuje dažnai vyrauja trumpalaikis požiūris, kai saugumo sprendimai finansuojami tik esant reguliaciniam spaudimui arba po incidentų, o ne kaip nuoseklios strategijos dalis.

Taktinis arba valdymo lygmuo patikslintame modelyje išlaikomas kaip jungtis tarp strateginių tikslų ir kasdienio įgyvendinimo, tačiau, remiantis ekspertų įžvalgomis, jis sustiprinamas tiekėjų valdymo, koordinavimo ir procedūrų suderinamumo aspektais.

Ekspertų interviu analizė parodė, kad praktikoje taktinis lygmuo dažnai tampa „siaurąja vieta“ kibernetinio saugumo valdyme. Net ir turint formaliai patvirtintas strategijas, jų įgyvendinimas stringa dėl nepakankamai aiškių, tarpusavyje nederančių arba fragmentiškai taikomų taktinių sprendimų. Strateginiai tikslai dažnai lieka aukšto lygio deklaracijomis, kurios ne visada transformuojamos į praktikoje veikiančias procedūras. Todėl patikslintame modelyje taktinis lygmuo sustiprinamas kaip organizacinė valdymo erdvė, kurioje politikos, procedūros, vaidmenys, tiekėjų valdymas ir koordinavimo mechanizmai turi būti aiškiai susieti su e. sveikatos sistemos procesais.

Operacinis lygmuo apima procesų vykdymą, incidentų registravimą, reagavimą, kontrolės priemones ir mokymąsi iš incidentų. Šis lygmuo yra kasdienės praktikos ir realaus saugumo įgyvendinimo erdvė. Būtent čia atsiskleidžia, ar strateginiai tikslai ir taktinės procedūros veikia realiomis sąlygomis. Mokslinėje literatūroje operacinis lygmuo siejamas su kasdieniu (angl. *frontline*) kibernetiniu saugumu, kuriame organizacinės taisyklės susiduria su naudotojų elgsena, darbo krūviu, technologiniais apribojimais ir klinikiniais prioritetais (Sarker ir kt., 2019).

Ekspertinio tyrimo rezultatai parodė, kad e. sveikatos sektoriuje būtent operaciniame lygmenyje dažnai išryškėja neatitikimai tarp formalių taisyklių ir realios praktikos. Incidentai ne visada registruojami sistemiškai, reagavimas dažnai apsiriboja techniniu sutrikimo pašalinimu, o išmoktos pamokos ne visuomet grįžta į rizikų vertinimo ar procedūrų atnaujinimo procesus. Todėl patikslintame modelyje operacinis lygmuo papildomas mokymosi iš incidentų elementu. Tai leidžia incidentus vertinti ne tik kaip sutrikimus, kuriuos reikia pašalinti, bet ir kaip duomenų šaltinį, padedantį tobulinti organizacinę saugumo brandą.

Technologinis lygmuo apima informacinių sistemų ir tinklų apsaugą, stebėseną, SIEM sprendimus, atsargines kopijas ir atkūrimą, tapatybių ir prieigų valdymą bei IoMT saugumą. Šis lygmuo sudaro techninį saugumo pagrindą, tačiau patikslintame modelyje jis nėra laikomas dominuojančiu. Mokslinėje literatūroje pažymima, kad vien technologinių sprendimų nepakanka užtikrinti atsparų kibernetinį saugumą, ypač sudėtingose socio-techninėse sistemose, tokiose kaip e. sveikatos infrastruktūra (von Solms ir van Niekerk, 2018; Sarker ir kt., 2019, Cichonski ir kt., 2018). Technologijos turi įgyvendinti strateginius ir taktinius sprendimus, bet neturi pakeisti valdymo.

Ekspertų interviu patvirtino, kad sveikatos sektoriuje technologinis lygmuo dažnai yra labiau išvystytas nei strateginis ar organizacinis. Dauguma organizacijų taiko bazines ar pažangesnes technines apsaugos priemones, tačiau jos neretai diegiamos fragmentiškai, be bendros saugumo architektūros vizijos. Todėl modelyje technologinis lygmuo siejamas su architektūriniu vientisumu, stebėsena, tapatybių ir prieigų kontrole, medicininių prietaisų saugumu ir atsarginių kopijų patikimumu. Šis lygmuo turi ne izoliuoti technologijas, bet integruoti jas į bendrą valdymo logiką.

Trečioji modelio zona – pagrindinės intervencijų ir valdymo dimensijos – yra centrinė empirinio modelio tikslinimo dalis. Ji apima devynias tarpusavyje susijusias dimensijas: strateginę integraciją, atsakomybių ir koordinavimo stiprinimą, rizikų valdymo brandą, incidentų valdymą ir mokymąsi, duomenų apsaugą ir privatumą, technologinę architektūrą ir stebėseną, tapatybių ir prieigų valdymą, saugumo kultūrą ir kompetencijas bei veiklos tęstinumą ir atsparumą.

Strateginė integracija reiškia, kad kibernetinis saugumas turi būti įtvirtintas kaip valdymo prioritetas ir suderintas su e. sveikatos sistemos tikslais. Ši dimensija reaguoja į ekspertų identifikuotą problemą, kad saugumas dažnai lieka formalaus atitikties ar techninių priemonių lygmenyje. Atsakomybių ir koordinavimo dimensija apima vaidmenų aiškumą ir tarpinstitucinį koordinavimą. Ji svarbi todėl, kad e. sveikatos sistemoje dalyvauja daug subjektų – sveikatos priežiūros įstaigos, nacionalinės informacinės sistemos valdytojai, IT paslaugų tiekėjai, priežiūros institucijos, sveikatos priežiūros specialistai ir pacientai.

Rizikų valdymo brandos dimensija patikslintame modelyje apima rizikų identifikavimą, analizę, vertinimą, prioritetų nustatymą ir nuolatinę stebėseną. Mokslinėje literatūroje pabrėžiama, kad rizikų valdymas sudaro kibernetinio saugumo valdymo ašį, leidžiančią organizacijoms racionaliai paskirstyti išteklius, nustatyti prioritetus ir priimti sprendimus esant neapibrėžtumui (Aven, 2016; NIST, 2023). E. sveikatos sektoriuje ši dimensija tampa ypač svarbi, nes kibernetinės rizikos gali turėti tiesioginį

poveikį pacientų saugai ir paslaugų tęstinumui.

Ekspertų interviu analizė parodė, kad daugelyje sveikatos sektoriaus organizacijų rizikų valdymas egzistuoja formaliai, tačiau menkai integruotas į realius sprendimų priėmimo procesus. Rizikų vertinimo dokumentai dažnai rengiami siekiant atitikti audito reikalavimus, tačiau jų rezultatai nėra sistemingai naudojami strateginiams prioritetams, finansavimo ar operaciniams veiksmams pagrįsti. Todėl patikslintame modelyje rizikų valdymas perkonstruojamas kaip aktyvus valdymo instrumentas, apimantis technines, organizacines ir klinikines rizikas. Toks požiūris atitinka tyrimus, kuriuose pabrėžiama, kad sveikatos sektoriaus kibernetinės rizikos negali būti vertinamos vien IT pažeidžiamumų požiūriu, nes jos persidengia su klinikiniais sprendimais, pacientų sauga ir paslaugų tęstinumu (Kruse ir kt., 2017; Jalali ir Kaiser, 2018; Coventry ir Branley, 2018).

Incidentų valdymo ir mokymosi dimensija apima incidentų aptikimą, reagavimą, atkūrimą ir išmoktas pamokas. Mokslinėje literatūroje incidentų valdymo efektyvumas kritinėse infrastruktūrose laikomas vienu svarbiausių veiksnių, lemiančių paslaugų tęstinumą ir visuomenės pasitikėjimą (Ahmad ir kt., 2014; Kohnke ir Sigler, 2016). E. sveikatos sistemose kibernetiniai incidentai dažnai peržengia technologinių trikdžių ribas ir sukelia platesnes organizacines bei klinikines pasekmes – nuo sutrikusios pacientų registracijos iki vėluojančių diagnostinių ar gydymo procesų.

Ekspertų interviu atskleidė, kad incidentų valdymas sveikatos sektoriuje dažnai apsiriboja techniniu atkūrimu. Po incidentų ne visada atliekama sisteminė analizė, apimanti ne tik technines, bet ir organizacines priežastis, komunikacijos spragas ar naudotojų elgseną. Todėl patikslintame modelyje incidentų valdymas siejamas su organizaciniu mokymusi. Išmoktos pamokos turi grįžti į rizikų vertinimą, politikų atnaujinimą, mokymus, pratybas ir techninių priemonių stiprinimą.

Duomenų apsaugos ir privatumo dimensija apima konfidencialumą, vientisumą, prieinamumą ir atsekamumą. E. sveikatos sistemoje ši dimensija yra viena svarbiausių, nes sveikatos duomenys yra jautrūs, o jų neteisėtas atskleidimas, pakeitimas ar neprieinamumas gali turėti ne tik teisinį, bet ir klinikinį poveikį. Šioje dimensijoje technologinės priemonės, tokios kaip šifravimas ar prieigos kontrolė, turi būti derinamos su organizacinėmis priemonėmis, naudotojų atsakomybėmis, audito mechanizmais ir teisės aktų reikalavimais. Vien techninis duomenų apsaugos sprendimas nėra pakankamas, jeigu nėra aiškiai apibrėžta, kas, kokiu pagrindu, kokiu tikslu ir kokiomis sąlygomis gali naudotis sveikatos duomenimis.

Technologinės architektūros ir stebėsenos dimensija apima segmentavimą, žurnalų analizę, SIEM, pažeidžiamumų valdymą ir bendros technologinės architektūros formavimą. Ši dimensija tiesiogiai reaguoja į ekspertų įvardytą technologinių sprendimų fragmentaciją. Sveikatos sektoriaus organizacijose technologijos dažnai diegiamos atskirais projektais, skirtingais finansavimo etapais ar pagal atskirų sistemų poreikius. Tai lemia saugumo priemonių dubliavimą, ribotą suderinamumą ir silpnesnį bendrą situacinį matomumą. Patikslintame modelyje technologinė architektūra suprantama kaip valdymo priemonė, leidžianti techninius sprendimus susieti su rizikomis, procesais ir atsakomybėmis.

Tapatybių ir prieigų valdymo dimensija apima MFA ir privilegijuotų prieigų kontrolę. Ši dimensija ypač svarbi e. sveikatos sektoriuje, nes prie sveikatos duomenų turi prieiti skirtingos naudotojų grupės: gydytojai, slaugytojai, vaistininkai, laboratorijų darbuotojai, administratoriai, pacientai ir techniniai specialistai. Netinkamai sukonfigūruotos ar laiku neperžiūrimos prieigos teisės yra viena iš reikšmingų saugumo pažeidimų priežasčių sveikatos sektoriuje (Abomhara ir Koien, 2015; Alshaikh, 2020). Todėl patikslintame modelyje prieigų valdymas traktuojamas ne kaip vienkartinė administracinė užduotis, o kaip nuolatinis kontrolės procesas, susietas su naudotojų vaidmenimis, atsakomybėmis ir veiklos poreikiais.

Saugumo kultūros ir kompetencijų dimensija apima mokymus, pratybas ir žmogiškojo veiksnio mažinimą. Ekspertai pabrėžė, kad žmogiškasis faktorius išlieka viena jautriausių kibernetinio saugumo grandžių. Todėl modelyje saugumo kultūra suprantama ne tik kaip formalūs mokymai, bet ir kaip darbuotojų atsakomybės suvokimas, vadovybės pavyzdys, praktinių grėsmių atpažinimas, saugaus elgesio įpročiai ir saugumo integravimas į kasdienius klinikinius bei administracinius procesus. Šis požiūris atitinka mokslinę literatūrą, kurioje saugumo kultūra laikoma būtina sąlyga efektyviam saugumo politikų įgyvendinimui (Puhakainen ir Siponen, 2010; Reason, 2016, He, Y. ir kt., 2021).

Veiklos tęstinumo ir atsparumo dimensija apima paslaugų tęstinumą. E. sveikatos kontekste atsparumas reiškia ne tik gebėjimą išvengti incidentų, bet ir gebėjimą išlaikyti kritines paslaugas, atkurti veiklą po sutrikimų ir mokytis iš incidentų. Ši dimensija ypač svarbi todėl, kad informacinių sistemų neprieinamumas sveikatos sektoriuje gali sutrikdyti pacientų registraciją, diagnostiką, receptų išrašymą, tyrimų rezultatų gavimą ir kitus klinikinius procesus. Todėl veiklos tęstinumas modelyje siejamas ne tik su techniniu atkūrimu, bet ir su organizaciniu pasirengimu, alternatyviomis darbo procedūromis ir komunikacijos mechanizmais.

Ketvirtoji modelio zona – integruojantis kibernetinio saugumo valdymo branduolys – yra modelio loginis centras. Jis sujungia valdymo lygmenis, intervencijų dimensijas, e. sveikatos sistemą, technines saugos priemones ir kritinio vertinimo mechanizmus. Branduolyje išskiriami penki principai: holistinis koordinavimas, duomenimis grįstas valdymas, pacientų sauga, e. sveikatos paslaugų patikimumas ir nuolatinis tobulinimas.

Siekiant išvengti normatyvinio modelio traktavimo, patikslintas modelis papildomai siejamas su operacinių kibernetinio atsparumo rodiklių logika. Tai reiškia, kad modelio poveikis e. sveikatos sistemos atsparumui neturi būti suprantamas kaip savaime atsirandantis rezultatas. Atsparumo didinimo prielaidos atsiskleidžia tik tada, kai modelio elementai yra susiejami su konkrečiais vertinimo požymiais: pasirengimo incidentams lygiu, incidentų aptikimo ir reagavimo laiku, paslaugų atkūrimo trukme, kritinių e. sveikatos paslaugų prieinamumu, atsarginių kopijų testavimo rezultatais, incidentų analizės po įvykio taikymu ir organizacinės brandos pokyčiais.

Todėl 9 paveiksle pateiktas modelis turi būti interpretuojamas ne tik kaip struktūrinė kibernetinio saugumo valdymo schema, bet ir kaip atsparumo vertinimo prielaidų sistema. Jo praktinis taikymas sudarytų galimybę rinkti ir analizuoti operacinius

rodiklius, tokius kaip vidutinis incidento aptikimo laikas, vidutinis reagavimo laikas, faktinis paslaugų atkūrimo laikas, kritinių paslaugų prieinamumo procentas, incidentų registravimo pilnumas, įgyvendintų korekcinių veiksmų dalis ir kibernetinio saugumo brandos vertinimo pokyčiai. Šie rodikliai leidžia modelio indėlį į atsparumą vertinti ne deklaratyviai, bet empiriškai patikrinamais požymiais.

Šie principai rodo, kad kibernetinio saugumo valdymas nėra atskirų procedūrų ar technologijų suma. Tai koordinavimo sistema, kurioje saugumas susiejamas su sveikatos paslaugų kokybe, duomenų apsauga, organizacine branda ir gebėjimu reaguoti į kintančias grėsmes.

Integruojantis branduolys taip pat leidžia paaiškinti modelio rodyklių logiką. Tiesioginės rodyklės žymi valdymo įtaką ir sprendimų judėjimą nuo strateginių nuostatų link operacinių bei technologinių veiksmų. Punktyrinės rodyklės žymi grįžtamąjį ryšį, kuriuo incidentų, audito, stebėsenos ir brandos vertinimo duomenys grąžinami į strateginio bei taktinio valdymo procesus. Dvikryptės rodyklės žymi sąveiką tarp e. sveikatos sistemos objektų, pavyzdžiui, tarp klinikinių procesų, sveikatos duomenų, sistemų sąveikos ir paslaugų tęstinumo. Integruojantys ryšiai parodo, kad atskiros saugumo priemonės turi veikti ne izoliuotai, bet kaip bendros valdymo sistemos dalis.

Penktoji modelio zona – kritinis vertinimas ir tobulinimas. Modelio stiprybėmis laikytini integruotas požiūris, e. sveikatos specifiškumas, valdymo lygių ir funkcijų suderinamumas bei ryšys su atsparumu. Integruotas požiūris leidžia išvengti siauro technologinio kibernetinio saugumo traktavimo. E. sveikatos specifiškumas užtikrina, kad modelis būtų susietas su pacientų sauga, klinikiniais procesais, sveikatos duomenimis, sistemų sąveika, medicininiais prietaisais ir paslaugų tęstinumu. Valdymo lygių ir funkcijų suderinamumas leidžia parodyti, kaip strateginiai sprendimai turi būti perkeliami į taktinius, operacinius ir technologinius veiksmus.

Kartu modelis turi ir ribotumų. Pirmasis ribotumas susijęs su įgyvendinimo kompleksiškumu. Modelis apima kelis valdymo lygmenis, devynias intervencijų dimensijas, išorinės reguliacinės aplinkos poveikį, technines priemones ir e. sveikatos sistemos saugomus objektus. Tokia struktūra leidžia tiksliau atspindėti e. sveikatos kibernetinio saugumo realybę, tačiau gali apsunkinti praktinį taikymą, ypač mažesnėse ar mažiau brandžiose organizacijose. Antrasis ribotumas yra priklausomybė nuo išteklių ir kompetencijų. Modeliui įgyvendinti reikalingi finansiniai, technologiniai, žmogiškieji ir vadybiniai pajėgumai, kurių skirtingos sveikatos priežiūros organizacijos gali turėti nevienodai. Trečiasis ribotumas susijęs su nevienoda organizacijų branda. Skirtingos įstaigos gali būti pasiekusios skirtingą kibernetinio saugumo lygį, todėl modelio taikymas negali būti vienodas visoms organizacijoms. Ketvirtasis ribotumas yra sudėtingas tarpinstitucinis koordinavimas, nes e. sveikatos sistema apima nacionalinę infrastruktūrą, lokalias informacines sistemas, išorinius tiekėjus ir skirtingų institucijų atsakomybes.

Tobulinimo mechanizmai modelyje siejami su brandos vertinimu, auditu ir rodikliais, grįžtamuoju ryšiu bei adaptavimu etapais. Brandos vertinimas leidžia nustatyti, kuriose srityse organizacija yra stipri, o kuriose reikalingos papildomos priemonės. Auditas ir rodikliai suteikia galimybę modelio taikymą grįsti ne vien ekspertiniu

vertinimu, bet ir stebimais duomenimis. Grįžtamasis ryšys leidžia incidentų, auditų, stebėsenos ir naudotojų informaciją grąžinti į strateginio bei taktinio valdymo procesus. Adaptavimas etapais reiškia, kad modelis neturi būti diegiamas kaip vienkartinė reforma. Jis turi būti taikomas pagal organizacijos brandą, prioritetus, turimus išteklius ir rizikų lygį.

Šeštoji modelio zona – e. sveikatos sistemos kontekstas ir saugomi objektai – parodo, kad modelis orientuotas ne į abstrakčią organizaciją, bet į specifinę e. sveikatos sistemą. Šioje zonoje išskiriami pacientų sauga, klinikiniai procesai, sveikatos duomenys, sistemų sąveika, ESPBI IS ir kitos informacinės sistemos, medicininiai prietaisai bei paslaugų tęstinumas. Šie elementai yra saugomi objektai, kurių patikimumas, prieinamumas, vientisumas ir atsparumas turi būti užtikrinami taikant kibernetinio saugumo valdymo priemones. Ši modelio dalis leidžia aiškiai parodyti, kad kibernetinio saugumo tikslas e. sveikatos sistemoje nėra vien sistemų ar duomenų apsauga, bet ir klinikinių paslaugų patikimumas, pacientų sauga bei visuomenės pasitikėjimas skaitmeninėmis sveikatos paslaugomis.

Papildomai modelyje išskiriama techninių saugos priemonių juosta: šifravimas, MFA, segmentavimas, žurnalų analizė, pažeidžiamumų valdymas, atsarginės kopijos ir atkūrimo testavimas. Šių priemonių įtraukimas sustiprina modelio technologinį pagrįstumą, tačiau jos sąmoningai pateikiamos ne kaip savarankiškas saugumo pagrindas, o kaip priemonės, palaikančios bendrą valdymo sistemą. Tai leidžia išvengti redukcinio požiūrio, kai kibernetinis saugumas suprantamas tik kaip techninių įrankių diegimas.

Modelio struktūrinis sudėtingumas yra sąmoningas ir pagrįstas e. sveikatos sistemos kompleksiškumu. E. sveikatos kibernetinis saugumas apima ne vien informacinių sistemų apsaugą, bet ir sveikatos duomenų gyvavimo ciklą, klinikinių procesų tęstinumą, pacientų saugą, medicininių prietaisų saugumą, naudotojų prieigas, tarpinstitucinį koordinavimą, reguliacinę atitiktį ir techninės infrastruktūros atsparumą. Todėl pernelyg supaprastintas modelis neleistų adekvačiai parodyti šių sąsajų. Vis dėlto pripažintina, kad sudėtinga modelio struktūra gali apsunkinti jo praktinį taikymą. Dėl šios priežasties modelyje įtrauktas kritinio vertinimo blokas ir numatomas etapinis adaptavimas.

Modelis remiasi mokslinės literatūros analize, tarptautinių standartų nuostatomis ir ekspertinio tyrimo rezultatais, todėl jo paskirtis yra konceptualiai struktūruoti kibernetinio saugumo valdymo lauką ir parodyti pagrindines tobulinimo kryptis. Modelis leidžia pagrįsti, kokios valdymo sritys turėtų būti stiprinamos. Modelio praktinis įgyvendinimas turi būti grindžiamas pradiniu organizacijos brandos ir rizikų vertinimu. Mažesnėms organizacijoms gali būti aktualu pirmiausia stiprinti tapatybių ir prieigų valdymą, atsarginių kopijų patikimumą, incidentų registravimą ir darbuotojų mokymus, o didesnėms organizacijoms – plėtoti SIEM, tiekėjų valdymą, veiklos tęstinumo testavimą ir tarpinstitucinio koordinavimo mechanizmus.

Modelio taikymo prielaidos taip pat yra svarbios. Modelis gali veikti tik tada, kai yra aiškus vadovybės įsitraukimas, paskirti atsakingi asmenys, apibrėžtos valdymo procedūros, inventorizuoti duomenų srautai ir informacinės sistemos, veikia

incidentų registravimo praktika, yra techninės stebėsenos pajėgumai ir vykdomas nuolatinis darbuotojų kompetencijų ugdymas. Be šių prielaidų modelis gali likti tik formaliu planavimo dokumentu, neturinčiu realaus poveikio kasdienei e. sveikatos sistemos saugumo praktikai.

Apibendrinant galima teigti, kad patikslintas kibernetinio saugumo valdymo modelis e. sveikatos sistemos tobulinimui išlaiko pradinio teorinio modelio daugialygę logiką, tačiau ją papildo empiriškai identifikuotomis intervencijų dimensijomis, techninėmis saugos priemonėmis, e. sveikatos sistemos saugomų objektų išskyrimu ir kritinio vertinimo bloku. Tokiu būdu modelis tampa ne tik konceptualiai išsamus, bet ir kritiškai pagrįstas. Jis leidžia parodyti, kokiais lygmenimis ir kokiomis priemonėmis turėtų būti stiprinamas e. sveikatos kibernetinis saugumas, kartu pripažįstant, kad modelio praktinis taikymas priklauso nuo organizacinės brandos, išteklių, kompetencijų ir tarpinstitucinio koordinavimo.

Taigi siūlomi struktūriniai ir funkciniai sprendimai sudaro integruotą kibernetinio saugumo valdymo modelio tikslinimo pagrindą. Jie tiesiogiai kyla iš ekspertinio tyrimo rezultatų ir sprendžia identifikuotas kritines sritis, išlaikydami aiškų ryšį su teorine analize ir e. sveikatos sistemos specifika. Dėl šios priežasties tolesniame poskyryje pagrįstai pereinama prie modelio adaptavimo praktiniam taikymui etapų, kurie leidžia sumažinti modelio įgyvendinimo kompleksiškumą ir taikyti jį nuosekliai, atsižvelgiant į konkrečios organizacijos brandą bei poreikius.

3.3.3. Patikslinto kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui adaptavimas praktiniam taikymui e. sveikatos sistemoje

Sukūrus ir struktūriškai patobulinus kibernetinio saugumo valdymo modelį remiantis ekspertinio tyrimo rezultatais, esminis disertacijos uždavinys tampa šio modelio adaptavimas praktiniam taikymui e. sveikatos sistemoje. Modelio adaptavimas šiame kontekste suprantamas ne kaip mechaninis teorinių sprendimų perkėlimas į organizacinę praktiką, bet kaip nuoseklus, etapinis ir jautrus procesas, leidžiantis integruoti siūlomą valdymo logiką į realiai egzistuojančias organizacines, technologines ir reguliacines struktūras.

Ekspertinio tyrimo rezultatai (žr. 3.2 ir 3.3.1 poskyrius) aiškiai parodė, kad e. sveikatos sistema pasižymi dideliu struktūriniu ir funkciniu nevienodumu. Dėl šios priežasties vieningo, universaliai taikomo vieno sprendimo visiems modelio įgyvendinimas būtų neefektyvus ir neatitiktų realių organizacijų galimybių. Todėl siūlomas kibernetinio saugumo valdymo modelis sąmoningai konstruojamas kaip adaptuojamas, modulinis ir grįstas brandos principu.

Modelio adaptavimas praktiniam taikymui grindžiamas trimis pagrindinėmis koncepcinėmis prielaidomis.

Pirma, e. sveikatos sistema yra socio-techninė sistema, kurioje technologiniai sprendimai yra neatsiejami nuo organizacinių struktūrų, žmogiškųjų veiksnių ir teisinio reguliavimo. Todėl modelio adaptavimas turi apimti ne tik techninių priemonių

diegimą, bet ir valdymo procesų, atsakomybių bei sprendimų priėmimo mechanizmų transformaciją.

Antra, modelio adaptavimas turi būti inkrementinis, t. y. įgyvendinamas palaipsniui, atsižvelgiant į organizacijos brandos lygį. Ekspertai ne kartą pabrėžė, kad bandymai iš karto įdiegti viską dažnai baigiasi formaliu atitikimu be realaus poveikio saugumui.

Trečia, modelio taikymas turi būti integruotas į esamus valdymo procesus, o ne funkcionuoti kaip atskira, izoliuota iniciatyva. Tai ypač aktualu sveikatos sektoriuje, kur dirba didelės organizacijos, tačiau turi ribotus resursus.

Praktinis modelio taikymas priklauso ne vien nuo nustatytų kibernetinio saugumo reikalavimų, bet ir nuo to, kaip jie įgyvendinami organizacijos valdymo procesuose. Ekspertinio tyrimo rezultatai parodė, kad viena svarbiausių problemų yra atotrūkis tarp formaliai nustatytų reikalavimų ir jų taikymo kasdienėje veikloje. Šiam atotrūkiui mažinti svarbūs keli tarpusavyje susiję vadybiniai mechanizmai: aiškus atsakomybių ir atskaitomybės paskirstymas, kibernetinių rizikų susiejimas su sprendimais dėl finansinių ir žmogiškųjų išteklių, nuoseklus padalinių bei institucijų veiksmų koordinavimas ir periodinė priimtų sprendimų įgyvendinimo stebėsena. Taikant modelį šie mechanizmai leidžia kibernetinio saugumo reikalavimus susieti su konkrečiais sprendimais, atsakingais subjektais ir jų įgyvendinimui reikalingais ištekliais, todėl kibernetinis saugumas tampa integralia organizacijos valdymo dalimi, o ne vien formalia atitikties funkcija.

Siekiant užtikrinti praktinį modelio taikomumą, jo adaptavimas siūlomas vykdyti trimis tarpusavyje susijusiais lygmenimis: instituciniu, organizaciniu ir operaciniu-technologiniu.

Instituciniame lygmenyje modelio adaptavimas siejamas su nacionalinio masto e. sveikatos ekosistemos valdymu. Ekspertų įžvalgos parodė, kad viena iš esminių problemų yra koordinacijos ir bendros krypties trūkumas tarp skirtingų institucijų.

Šiame lygmenyje modelio adaptavimas apima: bendrų kibernetinio saugumo valdymo principų įtvirtinimą e. sveikatos sistemos mastu; minimalių brandos reikalavimų nustatymą skirtingoms institucijų grupėms; informacijos apie grėsmes, incidentus ir gerąją praktiką apsikeitimo mechanizmų formalizavimą. Svarbu pabrėžti, kad modelis nenumato centralizuoto visų saugumo sprendimų valdymo. Priešingai, jis siūlo koordinuojamą decentralizaciją, kai institucijos išlaiko autonomiją, tačiau veikia bendrame metodologiniame ir informaciniame lauke.

Organizaciniame lygmenyje modelio adaptavimas yra orientuotas į konkrečių sveikatos sektoriaus organizacijų valdymo praktiką. Šiame lygmenyje modelis tampa praktiniu valdymo instrumentu, integruojamu į organizacijos strategiją, struktūrą ir kasdienę veiklą.

Adaptavimas šiame lygmenyje apima: kibernetinio saugumo funkcijos formalizavimą organizacijos struktūroje; aiškų atsakomybių paskirstymą tarp strateginio, taktinio ir operacinio lygmenų; rizikų ir incidentų valdymo procesų integravimą į bendrą organizacijos valdymo ciklą.

Ekspertinio tyrimo rezultatai rodo, kad organizacijos, kurios suvokia saugumą

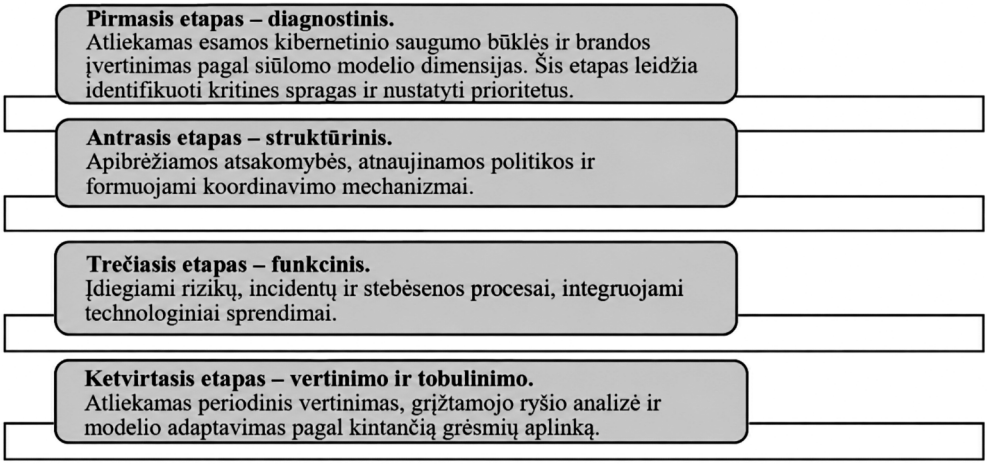
kaip organizacinę atsakomybę, pasižymi didesniu atsparumu ir greitesniu reagavimu į incidentus. Todėl modelio adaptavimas šiuo lygmeniu orientuotas į valdymo logikos pokytį, o ne vien procedūrų papildymą.

Operaciniame – technologiniame lygmenyje modelio adaptavimas susijęs su kasdienėmis saugumo praktikomis, technologinių sprendimų taikymu ir darbuotojų veiksmais. Ekspertai pabrėžė, kad būtent šiame lygmenyje dažniausiai išryškėja skirtumas tarp formalaus saugumo ir realios saugos.

Modelio adaptavimas šiame lygmenyje apima technologinių sprendimų integravimą į bendrą saugumo architektūrą; aiškių operacinių procedūrų taikymą incidentų atveju; nuolatinį darbuotojų sąmoningumo ugdymą.

Svarbu pažymėti, kad modelis nenumato vien tik technologijų diegimo. Jis pabrėžia technologijų, procesų ir žmonių sąveiką kaip esminį saugumo efektyvumo veiksnį.

Atsižvelgiant į ekspertų įžvalgas, siūlomas modelio adaptavimas vykdomas etapais (žr. 10 pav.).



10 pav. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui adaptavimo vykdymas etapais.

Šaltinis: sudaryta autorės

Atliekamas periodinis vertinimas, grįžtamojo ryšio analizė ir modelio adaptavimas pagal kintančią grėsmių aplinką. Modelio adaptavimas leidžia pasiekti kelis esminius rezultatus: pereiti nuo fragmentiško prie sisteminio saugumo valdymo; sustiprinti organizacinį atsparumą kibernetinėms krizėms; suderinti technologinius sprendimus su organizacinėmis realijomis; padidinti paslaugų tęstinumą ir pacientų pasitikėjimą.

Siekiant, kad modelio taikymas praktikoje nebūtų vertinamas vien formaliai, būtina numatyti operacinių kibernetinio atsparumo rodiklių stebėseną. Šie rodikliai leidžia nustatyti, ar modelio įgyvendinimas iš tiesų stiprina organizacijos pasirengimą, incidentų aptikimą, reagavimą, atkūrimą, paslaugų tęstinumą, mokymąsi ir organizacinę

brandą. Todėl praktinio modelio taikymo procese rekomenduotina taikyti pradinį vertinimą, periodinę stebėseną ir pakartotinį vertinimą po nustatyto laikotarpio.

Pradinis vertinimas turėtų būti atliekamas prieš diegiant modelio priemones. Jo metu nustatoma esama organizacijos būklė: ar atliekamas reguliarus rizikų vertinimas, ar veikia incidentų registravimo sistema, ar apibrėžti reagavimo procesai, ar testuojamos atsarginės kopijos, ar vertinamas kritinių paslaugų prieinamumas ir ar vykdomas brandos vertinimas. Šis pradinis matavimas sudarytų atskaitos tašką vėlesniam atsparumo pokyčio vertinimui.

Periodinė stebėsena turėtų būti siejama su konkrečiomis rodiklių grupėmis. Laiko rodikliai leistų vertinti incidentų aptikimo, reagavimo ir atkūrimo trukmę. Procesų rodikliai parodytų, ar organizacijoje realiai vykdomi rizikų vertinimai, incidentų registravimas, pratybos, atkūrimo testavimai ir veiklos tęstinumo plano peržiūros. Rezultatų rodikliai leistų vertinti kritinių paslaugų prieinamumą, neplanuotų sutrikimų trukmę, atsarginių kopijų testų rezultatus ir korekcinių veiksmų įgyvendinimą. Brandos ir valdymo rodikliai parodytų, ar kibernetinis atsparumas tampa integruota organizacinio valdymo dalimi.

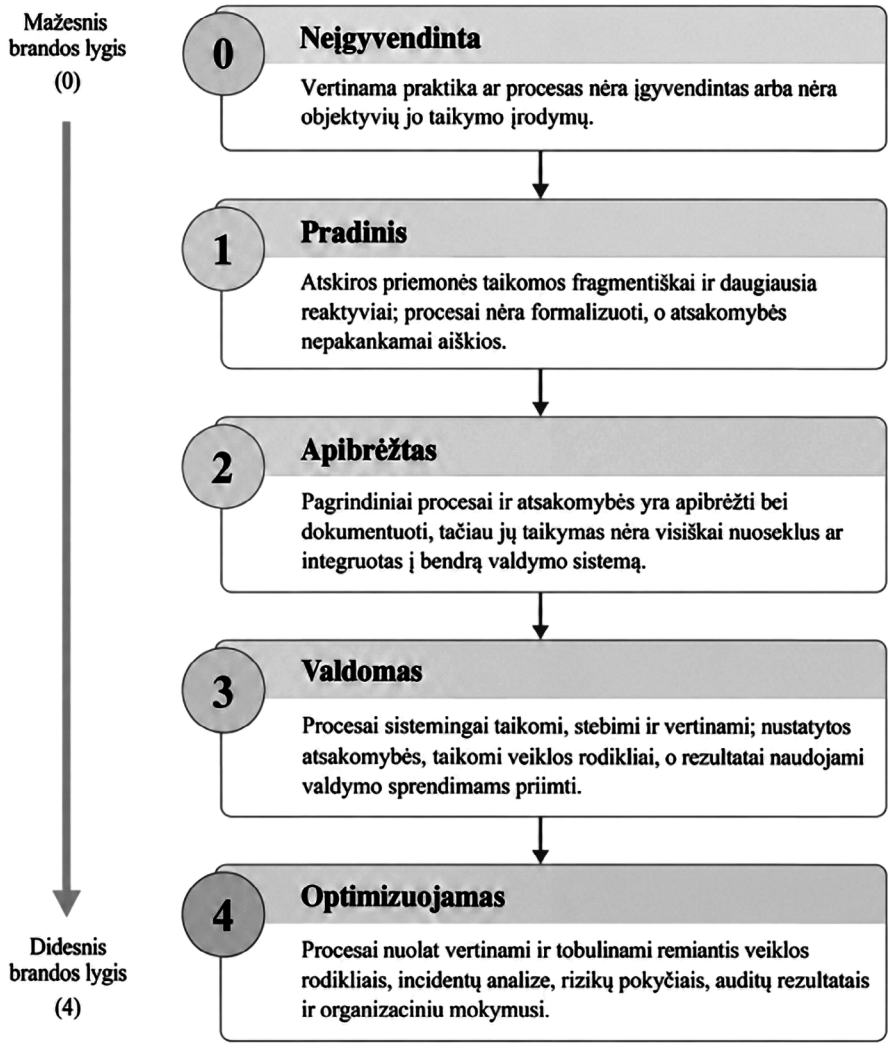
Pakartotinis vertinimas po modelio taikymo leistų palyginti pasirinktų rodiklių reikšmes su pradiniais duomenimis. Tokiu būdu būtų galima pagrįstai vertinti, ar sumažėjo incidentų aptikimo ir reagavimo laikas, ar pagerėjo paslaugų atkūrimo rodikliai, ar padidėjo kritinių e. sveikatos paslaugų prieinamumas, ar dažniau atliekamos analizės po incidentų ir ar didėja organizacijos kibernetinio saugumo branda.

Apibendrinant galima teigti, kad siūlomo kibernetinio saugumo valdymo modelio adaptavimas praktiniam taikymui e. sveikatos sistemoje grindžiamas integruotu ir etapiniu požiūriu. Modelis nėra statinis – jis numato nuolatinį tobulinimą, prisitaikymą prie kintančių grėsmių ir organizacijų brandos.

3.3.4. E. sveikatos kibernetinio saugumo valdymo brandos vertinimo metodika, grindžiama siūlomu modeliu

Siekiant sudaryti sąlygas patikslintą kibernetinio saugumo valdymo modelį taikyti ne tik kaip konceptualią valdymo struktūrą, bet ir kaip praktinį organizacijos kibernetinio saugumo valdymo būklės vertinimo instrumentą, parengta e. sveikatos kibernetinio saugumo valdymo brandos vertinimo metodika, grindžiama siūlomu modeliu. Metodika skirta sistemiškai įvertinti modelyje išskirtų valdymo lygmenų ir funkcinių dimensijų įgyvendinimo brandą, identifikuoti silpniausias valdymo sritis, nustatyti prioritetines tobulinimo kryptis ir sudaryti prielaidas periodiškai stebėti kibernetinio saugumo valdymo pažangą.

Kiekvienas vertinimo kriterijus vertinamas penkių lygių brandos skalėje nuo 0 iki 4. Skalė sudaryta taip, kad atspindėtų nuoseklų perėjimą nuo neįgyvendintų arba fragmentiškai taikomų kibernetinio saugumo valdymo praktikų iki sistemingai valdomų, matuojamų ir nuolat tobulinamų procesų. Vertinimas atliekamas remiantis organizacijos dokumentais, nustatytomis procedūromis, faktine jų taikymo praktika, atsakomybių paskirstymu ir turimais veiklos įrodymais.



11 pav. E. sveikatos kibernetinio saugumo valdymo brandos vertinimo skalė.

Šaltinis: sudaryta autorės

Vertinimas atliekamas pagal keturis pagrindinius valdymo lygmenis – strateginį, taktinį, operacinį ir technologinį – bei horizontaliąsias funkcines dimensijas, apimančias rizikų valdymą, incidentų valdymą, veiklos tęstinumą, atitiktį, darbuotojų kompetencijas ir nuolatinį tobulinimą.

Bendram e. sveikatos organizacijos kibernetinio saugumo valdymo brandos lygiui nustatyti apskaičiuojamas apibendrintas brandos indeksas. Jis gaunamas susumuojant

atskirų vertinimo kriterijų balus ir jų sumą dalijant iš vertinamų kriterijų skaičiaus. Visi kriterijai vertinami pagal vienodą 0–4 balų skalę, todėl šiame vertinimo modelyje jiems suteikiama vienoda reikšmė. Toks skaičiavimo principas pasirinktas siekiant užtikrinti vertinimo aiškumą, rezultatų palyginamumą ir išvengti papildomo subjektyvumo, kuris galėtų atsirasti atskiriems kriterijams priskiriant skirtingus svorius.

Bendras kibernetinio saugumo valdymo brandos indeksas apskaičiuojamas pagal formulę:

$$KSB = \frac{\sum_{i=1}^{n} x_i}{n}$$

KSB – bendras kibernetinio saugumo valdymo brandos indeksas;
$\mathbf{x_i}$ – konkrečiam vertinimo kriterijui suteiktas balas nuo 0 iki 4;
n – vertinamų kriterijų skaičius.

Taikant tą patį skaičiavimo principą gali būti nustatomas ir atskiro valdymo lygmens ar funkcinės dimensijos brandos indeksas. Tokiu atveju į skaičiavimą įtraukiami tik konkrečiai vertinamai sričiai priskirti kriterijai. Tai leidžia neapsiriboti vien bendru organizacijos brandos įverčiu, bet kartu nustatyti, kurios kibernetinio saugumo valdymo sritys yra labiau išplėtotos, o kurioms reikalingas didesnis organizacinis dėmesys ir tolesnis tobulinimas.

Apskaičiuota brandos indekso reikšmė interpretuojama pagal penkis kibernetinio saugumo valdymo brandos lygius. Kadangi atskiri kriterijai vertinami 0–4 balų skalėje, o bendras indeksas išreiškiamas jų vidurkiu, kiekvienam brandos lygiui priskiriamas atitinkamas reikšmių intervalas:

0,00–0,79 – neįgyvendinta. Kibernetinio saugumo valdymo praktikos iš esmės nėra įdiegtos arba jų taikymo organizacijoje negalima pagrįsti objektyviais įrodymais.

0,80–1,59 – pradinis lygis. Atskiros kibernetinio saugumo priemonės yra taikomos, tačiau jų įgyvendinimas išlieka fragmentiškas, daugiausia reaktyvus ir nepakankamai formalizuotas.

1,60–2,39 – apibrėžtas lygis. Pagrindiniai valdymo procesai, atsakomybės ir procedūros yra apibrėžti, tačiau jų praktinis taikymas dar nėra visiškai nuoseklus ir sistemiškai integruotas į organizacijos valdymą.

2,40–3,19 – valdomas lygis. Kibernetinio saugumo procesai organizacijoje taikomi sistemingai, jų vykdymas stebimas ir vertinamas, o gauti rezultatai naudojami priimant valdymo sprendimus.

3,20–4,00 – optimizuojamas lygis. Kibernetinio saugumo valdymas yra integruotas į organizacijos veiklą, procesai reguliariai vertinami, o jų tobulinimas grindžiamas veiklos rodikliais, rizikų pokyčiais, incidentų analize, auditų rezultatais ir organizaciniu mokymusi.

Toks rezultatų interpretavimas leidžia bendrą skaitinį įvertį susieti su konkrečia organizacijos kibernetinio saugumo valdymo būkle ir stebėti jos pokyčius atliekant periodinius vertinimus.

Praktiniam metodikos taikymui parengta kibernetinio saugumo valdymo brandos vertinimo matrica, kurioje modelio valdymo lygmenys ir funkcinės dimensijos susieti su konkrečiais vertinimo kriterijais, galimais vertinimo įrodymais ir nustatyta 0–4 balų brandos skale. Išsami vertinimo matrica pateikiama 7 priede. Toks vertinimo būdas sudaro galimybę nustatyti ne tik bendrą organizacijos kibernetinio saugumo valdymo brandos indeksą, bet ir atskirų modelio sričių brandą bei identifikuoti prioritetines tobulinimo kryptis.

3.4. Patikslinto kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui ekspertinis vertinimas

Šiame disertacijos poskyryje pateikiamas sukurto ir patikslinto kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui ekspertinis vertinimas, atliktas remiantis pusiau struktūruotų interviu su kibernetinio saugumo ir e. sveikatos srities ekspertais rezultatais. Ekspertinis vertinimas yra esminė dizaino mokslo tyrimų (angl. *Design Science Research*) metodologijos dalis, leidžianti empiriškai patikrinti, ar sukurtas artefaktas, šiuo atveju kibernetinio saugumo valdymo modelis, yra tinkamas, logiškai nuoseklus, praktiškai pritaikomas ir sprendžiantis identifikuotas problemas realiame kontekste.

Skirtingai nei ankstesniuose empirinio tyrimo etapuose, kuriuose buvo analizuojama esama saugumo būklė, identifikuojamos spragos ir kritinės valdymo sritys, šiame skyriuje dėmesys sutelkiamas į siūlomo modelio vertinimą kaip visumos, t. y. analizuojama, kaip ekspertai vertina jo struktūrą, funkcines dimensijas, adaptavimo logiką ir potencialą stiprinti e. sveikatos sistemos kibernetinį atsparumą.

3.4.1. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui tinkamumo ir taikymo galimybių vertinimas

Šiame poskyryje atliekamas nuodugnus sukurto kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui tinkamumo ir praktinio taikymo galimybių vertinimas, remiantis ekspertinio tyrimo rezultatais. Ekspertinis vertinimas yra esminė dizaino mokslo tyrimų (angl. *Design Science Research*) metodologijos dalis, nes leidžia empiriškai patikrinti, ar sukurtas artefaktas ne tik teoriškai pagrįstas, bet ir realiai pritaikomas konkrečiame socio-techniniame kontekste, šiuo atveju e. sveikatos sistemoje.

Skirtingai nei ankstesniuose empirinio tyrimo etapuose, kuriuose buvo analizuojama esama kibernetinio saugumo valdymo būklė, identifikuojamos sisteminės spragos ir kritinės valdymo sritys, šiame poskyryje dėmesys sutelkiamas į siūlomo modelio vertinimą kaip integruotos valdymo sistemos, kuri turi potencialą transformuoti fragmentuotą saugumo valdymą į nuoseklų, prevencinį ir brandos principais grįstą procesą.

Ekspertų buvo prašoma įvertinti, ar siūlomas kibernetinio saugumo valdymo modelis atitinka e. sveikatos sistemos veikimo realijas, įskaitant jos institucinį sudėtingumą, technologinį heterogeniškumą, teisinį reguliavimą ir informacinių sistemų

prieinamumo priklausomybę.

Didžioji dalis ekspertų vienareikšmiškai pabrėžė, kad siūlomas modelis iš esmės atitinka e. sveikatos sistemos prigimtį kaip sudėtingos, daugialypės ir aukštos rizikos socio-techninės sistemos.

Vienas ekspertas situaciją apibūdino taip:

„Tai nėra abstraktus modelis. Jis labai aiškiai atspindi, kaip realiai veikia e. sveikatos ekosistema – su daug veiksnių, skirtingais interesais ir priklausomybėmis“ (E1, asmeninis interviu, 2024-07-08).

Ekspertai akcentavo, kad modelio stiprybė slypi ne pavienių kontrolės priemonių ar procesų aprašyme, bet sisteminiame požiūryje, kuris leidžia suvokti kibernetinį saugumą kaip neatskiriamą sveikatos paslaugų teikimo dalį.

„Sveikatos sektoriuje saugumas negali būti atskira funkcija. Modelis tai labai aiškiai parodo“ (E6, asmeninis interviu, 2024-07-18).

Tokiu būdu modelis konceptualiai dera su ankstesniuose skyriuose aptartais socio-techniniais kibernetinio saugumo principais ir moderniomis saugumo valdymo paradigmomis, kurios pabrėžia organizacinių, technologinių ir žmogiškųjų veiksnių tarpusavio sąveiką.

Vienas esminių siūlomo modelio elementų – daugialypė valdymo struktūra, apimanti strateginį, organizacinį (taktinį) ir operacinį – technologinį lygmenis. Ekspertų vertinimu, būtent šis struktūrinis sprendimas daro modelį ypač tinkamą e. sveikatos sistemai.

Ekspertai pabrėžė, kad dabartinėje praktikoje kibernetinio saugumo sprendimai dažniausiai koncentruojami žemiausiame techniniame lygmenyje, ignoruojant strateginį ir organizacinį lygius.

„Dabar saugumas dažniausiai sprendžiamas serverių ir ugniasienių lygmenyje, bet ne valdymo lygmenyje“ (E4, asmeninis interviu, 2024-07-15).

Siūlomas modelis, pasak ekspertų, keičia šią logiką, nes aiškiai parodo, kad technologinės priemonės yra tik viena visumos dalis, o be strateginių sprendimų ir aiškaus atsakomybių paskirstymo jos negali užtikrinti ilgalaikio atsparumo.

„Modelis verčia pradėti nuo viršaus – nuo strategijos ir atsakomybės, o ne nuo technologijų pirkimo“ (E2, asmeninis interviu, 2024-07-09).

Ekspertai taip pat teigiamai vertino tai, kad modelyje numatyti grįžtamojo ryšio mechanizmai tarp skirtingų valdymo lygių, leidžiantys užtikrinti nuolatinį mokymąsi ir adaptaciją.

„Labai svarbu, kad modelis nėra linijinis, jis ciklišKas. Tai realiai atitinka, kaip turėtų veikti saugumo valdymas“ (E8, asmeninis interviu, 2024-07-23).

Vienas dažniausiai ekspertų akcentuotų aspektų – modelio pritaikomumas skirtingo dydžio ir brandos lygio sveikatos įstaigose. Ekspertai pabrėžė, kad e. sveikatos sistema nėra homogeniška, todėl bet koks valdymo modelis turi būti pakankamai lankstus.

„Negalime tikėtis, kad rajono ligoninė turės tokį patį saugumo lygį kaip universitetinė klinika“ (E7, asmeninis interviu, 2024-07-22).

Ekspertų nuomone, siūlomas modelis yra modulinis, todėl leidžia jį diegti etapais, pradedant nuo kritinių komponentų.

„Man patinka, kad modelį galima naudoti kaip kelio žemėlapį – nereikia visko iš karto“ (E5, asmeninis interviu, 2024-07-16).

Tai ypač svarbu viešojo sektoriaus kontekste, kuriame organizacijos dažnai susiduria su ribotais finansiniais ir žmogiškaisiais resursais.

Ekspertai taip pat pabrėžė, kad modelis gali būti naudojamas ne tik kaip įgyvendinimo įrankis, bet ir kaip įsivertinimo bei brandos diagnostikos pagrindas.

„Pagal šį modelį galima labai aiškiai matyti, kur organizacija yra ir kur ji nori nueiti“ (E9, asmeninis interviu, 2024-07-25).

Vertinant modelio taikymo galimybes, ekspertai daug dėmesio skyrė jo suderinamumui su BDAR, TIS2 direktyva ir nacionaliniais kibernetinio saugumo reikalavimais.

Ekspertų nuomone, modelis nėra konkurencinis esamiems reguliaciniams reikalavimams, bet veikiau juos sujungia.

„Reglamentai pasako, ką reikia padaryti, o šis modelis parodo, kaip tai padaryti“ (E3, asmeninis interviu, 2024-07-11).

Ekspertai pažymėjo, kad praktikoje dažnai trūksta būtent šios jungties tarp teisės aktų ir kasdienės veiklos, o siūlomas modelis gali veikti kaip tarpinis valdymo mechanizmas.

Nepaisant bendro teigiamo vertinimo, ekspertai taip pat identifikavo realius modelio taikymo apribojimus. Vienas svarbiausių – vadovybės įsitraukimo trūkumo rizika.

„Jeigu vadovybė nepriims modelio kaip strateginio dokumento, jis liks stalčiuje“ (E3, asmeninis interviu, 2024-07-11).

Kitas apribojimas – riboti žmogiškieji resursai, ypač mažesnėse įstaigose.

„Modelis reikalauja kompetencijų, kurių ne visur yra“ (E6, asmeninis interviu, 2024-07-18).

Tačiau ekspertai pabrėžė, kad šie apribojimai nėra modelio trūkumai, o sisteminės e. sveikatos sektoriaus problemos, kurias pats modelis padeda identifikuoti.

Ekspertų vertinimų suderinamumui nustatyti taikytas Kendall konkordacijos koeficientas W. Šis koeficientas naudojamas kelių vertintojų, vertinančių tuos pačius objektus ar kriterijus, ranginių vertinimų suderinamumui įvertinti. Kendall W apskaičiuojamas remiantis rangų sumų nuokrypiais nuo vidutinės rangų sumos, o jo reikšmė svyruoja nuo 0 iki 1, kai 0 reiškia suderinamumo nebuvimą, o 1 – visišką vertinimų sutapimą (Legendre, 2022).

Pateikiamas bendras ekspertų vertinimų suderinamumo skaičiavimas, susijęs su kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui vertinimo kriterijais.

Toliau pateikiami Kendall konkordacijos koeficiento skaičiavimai. Tyrime 9 ekspertai vertino 9 kibernetinio saugumo valdymo modelio kriterijus. Kiekvienas ekspertas kriterijams suteikė rangus nuo 1 iki 9, kur 1 reiškia aukščiausią reikšmingumą, o 9 – mažiausią reikšmingumą. Kadangi ekspertų rangavimuose sutampančių rangų nebuvo, papildoma sutapusių rangų korekcija netaikyta.

16 lentelė. Vertinimo kriterijai

Kriterijaus kodas	Vertinimo kriterijus
K1	Modelio struktūros aiškumas
K2	Modelio loginis nuoseklumas
K3	Modelio pritaikomumas e. sveikatos sistemos kontekste
K4	Rizikų valdymo dimensijos pagrįstumas
K5	Incidentų valdymo dimensijos pagrįstumas
K6	Atsakomybių paskirstymo aiškumas
K7	Modelio tinkamumas organizaciniam pasirengimui stiprinti
K8	Modelio praktinio taikymo galimybės
K9	Modelio tinkamumas kibernetinio saugumo brandai vertinti

Šaltinis: sudaryta autorės

17 lentelė. Ekspertų suteikti rangai

Ekspertas	K1	K2	K3	K4	K5	K6	K7	K8	K9
E1	4	9	2	1	5	7	3	6	8
E2	9	7	3	4	1	2	6	5	8
E3	5	8	1	2	3	4	6	7	9
E4	5	8	3	7	4	2	1	6	9
E5	6	8	1	4	3	2	5	7	9
E6	6	8	3	2	4	1	5	7	9
E7	6	3	4	7	1	5	2	8	9
E8	4	8	3	5	1	2	7	6	9
E9	6	7	2	3	1	4	5	8	9
Rangų suma Rj	**51**	**66**	**22**	**35**	**23**	**29**	**40**	**60**	**79**

Šaltinis: sudaryta autorės

Pagal rangų sumas matyti, kad mažiausią rangų sumą gavo K3 ir K5 kriterijai. Kadangi mažesnis rangas reiškia didesnį reikšmingumą, tai rodo, kad ekspertai labiausiai išskyrė modelio pritaikomumą e. sveikatos sistemos kontekste ir incidentų valdymo dimensijos pagrįstumą. Taip pat santykinai reikšmingai įvertintas atsakomybių paskirstymo aiškumas, kurio rangų suma siekė 29.

Kendall konkordacijos koeficientas apskaičiuojamas pagal formulę:

$W = 12S / [m^2(n^3 - n)]$

W – Kendall konkordacijos koeficientas;

m – ekspertų skaičius;

n – vertinamų kriterijų skaičius;

S – rangų sumų nuokrypių nuo vidutinės rangų sumos kvadratų suma.

Šiuo atveju: m = 9; n = 9

Pirmiausia apskaičiuojama vidutinė rangų suma:

$\tilde{R} = m(n + 1) / 2$

$\tilde{R} = 9(9 + 1) / 2 = (9 \times 10) / 2 = 45$

Taigi:

$\tilde{R} = 45$

Toliau apskaičiuoti kiekvieno kriterijaus rangų sumų nuokrypiai nuo vidutinės rangų sumos.

18 lentelė. Rangų sumų nuokrypių skaičiavimas

Kriterijus	**Rangų suma Rj**	**Rj – $\tilde{R}$**	**$(Rj - R)^2$**
K1	51	6	36
K2	66	21	441
K3	22	-23	529
K4	35	-10	100
K5	23	-22	484
K6	29	-16	256
K7	40	-5	25
K8	60	15	225
K9	79	34	1156
Iš viso S			**3252**

Šaltinis: sudaryta autorės

Apskaičiuota rangų sumų nuokrypių kvadratų suma: S = 3252

Tuomet apskaičiuotas Kendall konkordacijos koeficientas:

$W = (12 \times 3252) / [9^2(9^3 - 9)]$

$W = 39024 / [81(729 - 9)]$

$W = 39024 / (81 \times 720)$

$W = 39024 / 58320$

$W = 0{,}669$

Gautas Kendall konkordacijos koeficientas: W = 0,669

Kendall W reikšmingumui patikrinti taikytas chi kvadrato kriterijus:

$\chi^2 = m(n - 1)W$

$\chi^2 = 9(9 - 1) \times 0{,}669$

$\chi^2 = 9 \times 8 \times 0{,}669$

$\chi^2 = 48{,}18$

Laisvės laipsnių skaičius:

df = n − 1

df = 9 − 1 = 8

Pagal chi kvadrato skirstinį, kai: $\chi^2 = 48{,}18$ ir: df = 8 gauta reikšmė yra statistiškai reikšminga: $p < 0{,}001$

Apskaičiuotas Kendall konkordacijos koeficientas yra: W = 0,669

Tai rodo stiprų ekspertų vertinimų suderinamumą. Kadangi p reikšmė yra mažesnė nei 0,05, galima teigti, kad ekspertų vertinimų suderinamumas yra statistiškai reikšmingas.

Tai reiškia, kad ekspertų vertinimai dėl kibernetinio saugumo valdymo modelio kriterijų nėra atsitiktiniai ar tarpusavyje nesuderinti. Priešingai, jų vertinimuose matomas pakankamai aiškus sutarimas dėl to, kurie modelio kriterijai yra reikšmingesni. Labiausiai išskirti kriterijai yra modelio pritaikomumas e. sveikatos sistemos kontekste, incidentų valdymo dimensijos pagrįstumas ir atsakomybių paskirstymo aiškumas.

Remiantis atliktais skaičiavimais, galima daryti išvadą, kad ekspertų vertinimai yra pakankamai suderinti, todėl jų pagrindu galima formuluoti apibendrintas išvadas apie kibernetinio saugumo valdymo modelio tinkamumą, struktūrinį nuoseklumą ir praktinio taikymo galimybes tyrimo imties ribose.

Apibendrintai galima teigti, kad ekspertų vertinimų suderinamumui įvertinti buvo taikytas Kendall konkordacijos koeficientas W. Ekspertai vertino tuos pačius kibernetinio saugumo valdymo modelio kriterijus, suteikdami jiems rangus pagal reikšmingumą. Atlikus skaičiavimus nustatyta, kad Kendall konkordacijos koeficientas siekia W = 0,669. Tai rodo stiprų ekspertų vertinimų suderinamumą. Chi kvadrato kriterijaus reikšmė $\chi^2 = 48{,}18$, kai df = 8, o $p < 0{,}001$, patvirtina, kad ekspertų vertinimų suderinamumas yra statistiškai reikšmingas. Todėl galima teigti, kad ekspertų vertinimai dėl modelio kriterijų yra pakankamai nuoseklūs ir gali būti naudojami apibendrintoms išvadoms formuluoti tyrimo imties ribose.

Ekspertinis vertinimas patvirtina siūlomo kibernetinio saugumo valdymo modelio konceptualinį pagrįstumą, struktūrinį nuoseklumą ir praktinį pritaikomumą e. sveikatos sistemos kontekste. Modelis vertinamas kaip tinkamas spręsti identifikuotas saugumo valdymo problemas, suderinamas su reguliaciniu kontekstu ir pakankamai lankstus skirtingo brandos lygio organizacijoms.

Ekspertų įžvalgos taip pat atskleidė, kad modelio sėkmė priklauso ne tik nuo jo struktūros, bet ir nuo organizacinių bei institucinės aplinkos veiksnių, ypač vadovybės įsitraukimo ir ilgalaikio požiūrio į kibernetinį saugumą.

Šios išvados sudaro tvirtą empirinį pagrindą kitame poskyryje (3.4.2) detaliau analizuoti modelio stiprybes, ribotumus ir tobulinimo kryptis, siekiant dar labiau padidinti jo praktinę vertę ir taikomumą e. sveikatos sistemoje.

3.4.2. Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui stiprybės, ribotumai ir strateginės kryptys

Šiame poskyryje atliekama kritinė siūlomo kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui analizė, siekiant sistemiškai įvertinti jo stiprybes, identifikuoti galimus ribotumus bei suformuluoti pagrįstas tobulinimo kryptis. Toks

vertinimas yra esminė dizaino mokslo tyrimų (angl. *Design Science Research*) metodologijos dalis, nes leidžia ne tik patvirtinti sukurto artefakto vertę, bet ir aiškiai apibrėžti jo taikymo ribas bei sąlygas, kuriomis modelis gali būti toliau adaptuojamas ir plėtojamas (Hevner ir kt., 2004; Peffers ir kt., 2007).

Skirtingai nei ankstesniame poskyryje, kuriame buvo analizuojamas bendras modelio tinkamumas ir taikymo galimybės e. sveikatos sistemoje, šiame etape dėmesys sutelkiamas į analitinę sintezę, jungiančią ekspertų įžvalgas, identifikuotas sistemines problemas (3.2.), kritines kibernetinio saugumo valdymo sritis (3.3.), ir dizaino mokslo principus.

Tokiu būdu šis poskyris sujungia empirinio tyrimo rezultatus ir galutines disertacijos išvadas bei rekomendacijas.

Viena reikšmingiausių siūlomo kibernetinio saugumo valdymo modelio stiprybių – jo sisteminė ir integruota struktūra, leidžianti vertinti kibernetinį saugumą ne kaip izoliuotų techninių priemonių rinkinį, bet kaip visumą, apimančią strateginius, organizacinius, procesinius, technologinius ir žmogiškuosius aspektus.

Ekspertinio tyrimo rezultatai parodė, kad būtent tokio holistinio požiūrio labiausiai trūksta dabartinėje e. sveikatos sistemos praktikoje. Modelis konceptualiai atsako į šią problemą, nes aiškiai apibrėžia skirtingų valdymo lygių vaidmenis ir jų tarpusavio sąveiką.

Mokslinėje literatūroje pabrėžiama, kad kibernetinio saugumo problemos sudėtingose socio-techninėse sistemose negali būti sprendžiamos vien technologinėmis priemonėmis (Sarker ir kt., 2019). Siūlomas modelis atitinka šią paradigmą, nes integruoja organizacinę atsakomybę, sprendimų priėmimo mechanizmus ir technologinę infrastruktūrą į vientisą valdymo sistemą.

Kita reikšminga stiprybė – aiški modelio sąsaja su kibernetinio saugumo brandos vertinimo logika. Modelis nėra statiškas – jis leidžia organizacijoms identifikuoti savo esamą brandos lygį ir kryptingai planuoti tolesnį tobulėjimą.

Tai ypač aktualu e. sveikatos sektoriuje, kuriame organizacijų brandos lygis labai skiriasi. Brandos principų integravimas leidžia modelį taikyti kaip diagnostinį įrankį, strateginį planavimo instrumentą, ir nuolatinio tobulinimo (angl. *continuous improvement*) pagrindą.

Tokį požiūrį palaiko ir tarptautiniai standartai, pavyzdžiui, ISO/IEC 27001, kuriuose akcentuojamas PDCA ciklo taikymas informacijos saugumo valdyme. Ekspertai taip pat pabrėžė modelio praktinį orientavimą. Skirtingai nei daugelis teorinių modelių, siūlomas sprendimas leidžia organizacijoms pasirinkti prioritetines sritis ir diegti modelį etapais.

Modulinė struktūra laikytina reikšminga stiprybe, nes mažina įgyvendinimo riziką, leidžia prisitaikyti prie ribotų resursų, ir sudaro sąlygas palaipsniui didinti saugumo brandą.

Nepaisant identifikuotų stiprybių, ekspertinis vertinimas taip pat atskleidė tam tikrus modelio ribotumus, kuriuos būtina kritiškai įvertinti.

Vienas pagrindinių ribotumų – modelio veiksmingumo priklausomybė nuo organizacinės brandos lygio. Nors modelis yra lankstus, jo sėkmingas taikymas reikalauja

bent minimalaus vadovybės įsitraukimo, saugumo atsakomybės pasidalinimo, ir organizacinės disciplinos.

Organizacijose, kuriose šie elementai neegzistuoja, modelio įgyvendinimas gali būti fragmentiškas arba formaliai imitacinis. Ekspertai taip pat nurodė, kad modelis numato aiškias funkcijas ir atsakomybes, tačiau praktikoje daugelyje sveikatos įstaigų trūksta kompetentingų specialistų.

Tai reiškia, kad modelio struktūra gali būti teisinga, tačiau jos įgyvendinimas susidurs su žmogiškųjų resursų trūkumu. Modelis konceptualiai numato tarpinstitucinę sąveiką, tačiau jos įgyvendinimas priklauso nuo platesnio nacionalinio koordinavimo mechanizmų, kurie ne visada yra pakankamai išvystyti. Tai riboja modelio poveikį sisteminiu mastu ir reikalauja papildomų sprendimų nacionalinės politikos lygmeniu.

Toliau pateikiama 19 lentelė, apibendrinanti pagrindines identifikuotas stiprybes, ribotumus ir galimas tobulinimo kryptis.

19 lentelė. Patikslinto kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui stiprybių, ribotumų ir strateginių krypčių sintezė

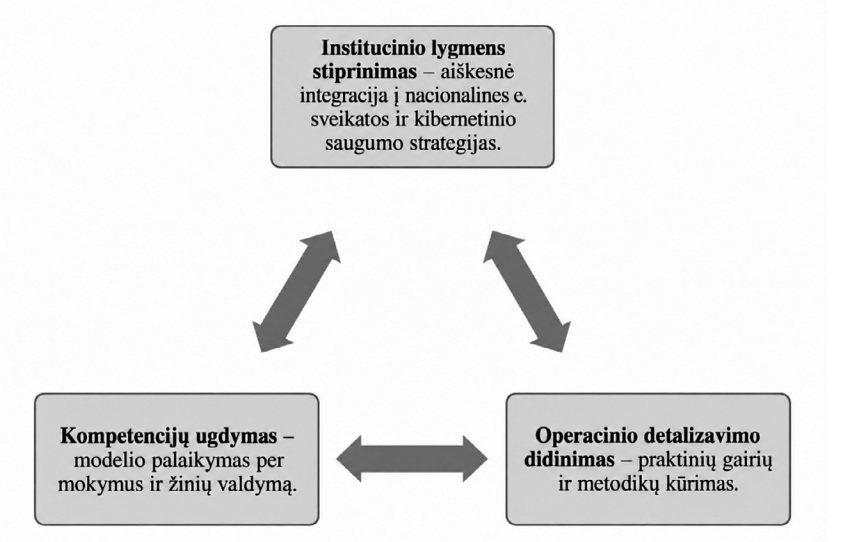
Analitinė dimensija	Identifikuotos stiprybės	Nustatyti ribotumai	Siūlomos strateginės kryptys
Strateginis valdymas	Integruotas į organizacijos valdymo struktūrą	Priklausomas nuo vadovybės įsitraukimo	Formalizuoti privalomą vadovybės vaidmenį
Organizacinė struktūra	Aiškus atsakomybių paskirstymas	Trūksta kompetentingų specialistų	Kurti kompetencijų ugdymo programas
Rizikų valdymas	Brandos principais grįsta logika	Dažnai formaliai taikomas	Integruoti rizikas į sprendimų priėmimą
Incidentų valdymas	Numatyti grįžtamojo ryšio ciklai	Ribota praktinė patirtis	Reguliarūs pratybų scenarijai
Technologinis saugumas	Neatsiejamas nuo organizacinio lygmens	Fragmentuota infrastruktūra	Centralizuota architektūrinė vizija
Tarpinstitucinė sąveika	Modeliuojama koncepciniu lygmeniu	Priklauso nuo nacionalinės politikos	Nacionalinio koordinavimo stiprinimas

Šaltinis: sudaryta autorės, remiantis ekspertinio tyrimo rezultatais

Identifikuotos tobulinimo kryptys neturėtų būti interpretuojamos kaip modelio silpnybės, bet veikiau kaip natūralios dizaino mokslo tyrimų proceso dalys, kuriose modelis toliau evoliucionuoja.

Remiantis Hevner ir kt. (2004), dizaino artefaktai yra objektai, kurie turi būti nuolat testuojami, adaptuojami ir tobulinami keičiantis kontekstui.

Ekspertų įžvalgos leidžia išskirti tris pagrindines modelio plėtros kryptis:



12 pav. Pagrindinės kibernetinio saugumo modelio e. sveikatos sistemos tobulinimui plėtros kryptys.

Šaltinis: sudaryta autorės

Apibendrinant galima teigti, kad siūlomas kibernetinio saugumo valdymo modelis e. sveikatos sistemos tobulinimui pasižymi reikšmingomis konceptualiomis ir praktinėmis stiprybėmis, kurios leidžia jį laikyti tinkamu e. sveikatos sistemos tobulinimo instrumentu. Identifikuoti ribotumai nėra kritiniai ir daugeliu atvejų atspindi platesnes sistemines sveikatos sektoriaus problemas, o ne paties modelio trūkumus.

Ekspertinio vertinimo pagrindu suformuluotos tobulinimo kryptys sudaro pagrindą tolesniam modelio adaptavimui ir praktiniam įgyvendinimui, taip pat atveria galimybes ateities moksliniams tyrimams.

20 lentelė. Tiriamųjų klausimų (TK1–TK4) analizės rezultatų apibendrinimas

Tiriamasis klausimas	Taikytas analizės būdas	Empirinio atsakymo pagrindas	Apibendrintas atsakymas
TK1	Teminė analizė, fragmentiškumo kategorijų matrica, Kendall W	Ekspertų pasisakymuose kartojasi techninio požiūrio dominavimas, atsakomybių neaiškumas ir rizikų valdymo fragmentiškumas	TK1 analizė atskleidė kibernetinio saugumo valdymo fragmentiškumo požymius e. sveikatos organizacijose.
TK2	Teminė analizė, integruoto valdymo elementų ribotumo analizė, Kendall W	Ekspertai nurodo nepakankamą strateginio, taktinio, operacinio ir technologinio lygmenų integraciją	TK2 analizė atskleidė ribotą strateginio, taktinio, operacinio ir technologinio kibernetinio saugumo valdymo lygmenų integraciją e. sveikatos organizacijose.
TK3	Teminė sąsajų analizė, incidentų valdymo kategorijų matrica, Kendall W	Ekspertų pasisakymuose struktūrizuotas valdymas siejamas su aiškesniu incidentų valdymu	TK3 analizė parodė, kad ekspertai kibernetinio saugumo valdymo struktūrizuotumą sieja su veiksmingesniu incidentų valdymu e. sveikatos organizacijose.
TK4	Ekspertinis modelio validavimas, poveikio organizaciniam pasirengimui kategorijų analizė, Kendall W	Ekspertai siūlomo modelio elementus sieja su geresniu organizaciniu pasirengimu kibernetinėms grėsmėms ir nuoseklesniu kibernetinio saugumo valdymu.	TK4 analizė parodė, kad ekspertai siūlomą kibernetinio saugumo valdymo modelį sieja su galimybėmis stiprinti organizacinį pasirengimą kibernetinėms grėsmėms e. sveikatos sistemos kontekste.

Šaltinis: sudaryta autorės, remiantis ekspertinio tyrimo duomenimis (N = 9)

Atsakant į TK1 nustatyta, kad ekspertų vertinimu kibernetinio saugumo valdymo fragmentiškumas e. sveikatos organizacijose pasireiškia ne tik technologinių priemonių taikymo trūkumais, bet ir organizacinio bei vadybinio pobūdžio problemomis. Ekspertų pasisakymuose išryškėjo techninio požiūrio dominavimas, nepakankamai aiškus atsakomybių paskirstymas, nenuoseklus rizikų valdymas ir ribotas grįžtamasis ryšys po kibernetinių incidentų.

TK2 analizė parodė, kad integruoto kibernetinio saugumo valdymo elementai e. sveikatos organizacijose taikomi nevienodai ir ne visais atvejais sudaro nuoseklią tarpusavyje susietą valdymo sistemą. Ekspertų vertinimuose išryškėjo strateginio, taktinio, operacinio ir technologinio valdymo lygmenų sąveikos trūkumai, rodantys nepakankamą kibernetinio saugumo integraciją į bendrą organizacijos valdymo sistemą.

TK3 analizės rezultatai atskleidė, kad ekspertai struktūrizuotą kibernetinio saugumo valdymą sieja su nuoseklesniu incidentų valdymo procesu, aiškiau apibrėžtomis atsakomybėmis ir veiksmingesniu reagavimu į kibernetinius incidentus e. sveikatos organizacijose.

TK4 analizės rezultatai atskleidė, kad ekspertai siūlomo kibernetinio saugumo valdymo modelio elementus sieja su nuoseklesniu kibernetinio saugumo valdymu, geresniu organizaciniu pasirengimu kibernetinėms grėsmėms ir didesniu organizacijų atsparumu galimiems kibernetiniams incidentams.

Apibendrinant galima teigti, kad atlikta ekspertinių interviu analizė sudarė galimybę nuosekliai atsakyti į visus keturis disertacijoje suformuluotus tiriamuosius klausimus. Tyrimo rezultatai atskleidė, kad e. sveikatos kibernetinio saugumo valdymas turėtų būti vertinamas kaip integruotas organizacinis procesas, apimantis strateginius sprendimus, aiškų atsakomybių paskirstymą, nuoseklų rizikų ir incidentų valdymą, technologines priemones bei nuolatinio tobulinimo mechanizmus.

IŠVADOS

1. Teorinė analizė parodė, kad e. sveikatos kibernetinio saugumo valdymas yra kompleksinis socio-techninis ir vadybinis reiškinys, kurio veiksmingumą lemia ne pavienės kontrolės priemonės, o strateginių, organizacinių, procesinių ir technologinių sprendimų tarpusavio sąveika. Todėl kibernetinis saugumas turi būti integruojamas į bendrą organizacijos valdymo sistemą, siejant jį su atsakomybių paskirstymu, rizikų valdymu, veiklos tęstinumu ir nuolatiniu brandos didinimu.
   1.1. E. sveikatos sistemos kibernetinio saugumo valdymo kompleksiškumą lemia informacinių sistemų tarpusavio priklausomybė, jautrių sveikatos duomenų srautai ir skirtingų organizacijų atsakomybės ribos. Teorinė analizė parodė, kad vien techninėmis kontrolės priemonėmis ar formalia atitiktimi grindžiamas požiūris nėra pakankamas, nes kibernetinio saugumo rezultatus lemia ir rizikų valdymo, atsakomybių paskirstymo, incidentų valdymo, veiklos tęstinumo bei nuolatinio tobulinimo procesų tarpusavio sąveika.
   1.2. Teorinė analizė parodė, kad tarptautiniai standartai, informacijos saugumo valdymo sistemos, rizikų valdymo metodikos ir brandos modeliai sudaro reikšmingą metodinį pagrindą, tačiau jų taikymas e. sveikatos sistemoje reikalauja papildomo vadybinio pritaikymo. Šiame kontekste esminę reikšmę įgyja ne tik technologinių ir duomenų apsaugos reikalavimų įgyvendinimas, bet ir jų susiejimas su tarpinstituciniu koordinavimu, atsakomybių paskirstymu, veiklos tęstinumo valdymu ir nuosekliu kibernetinio atsparumo stiprinimu.
   1.3. Teorinė analizė pagrindė integruoto kibernetinio saugumo valdymo poreikį, kai strateginiai, organizaciniai, procesiniai ir technologiniai sprendimai siejami tarpusavyje, o ne įgyvendinami kaip atskiros saugumo priemonės. Vadybiniu požiūriu esminę reikšmę įgyja aiškus atsakomybių paskirstymas, rizikomis grindžiamas sprendimų priėmimas, skirtingų valdymo lygmenų koordinavimas ir nuolatinis procesų vertinimas bei tobulinimas.
2. Sisteminė e. sveikatos sistemų kibernetinių incidentų ir atakų analizė parodė, kad kibernetinio atsparumo pažeidžiamumą lemia kompleksinė technologinių, organizacinių, procesinių ir žmogiškųjų veiksnių sąveika. Todėl incidentų valdymo veiksmingumas priklauso ne tik nuo techninių apsaugos priemonių, bet ir nuo organizacijos gebėjimo integruoti rizikų vertinimą, reagavimą, veiklos atkūrimą ir organizacinį mokymąsi į nuoseklų valdymo procesą.
   2.1. Sisteminė incidentų ir atakų analizė atskleidė, kad jų poveikio mastą e. sveikatos sistemoje lemia ne vien techninis pažeidimo pobūdis, bet ir kritinių paslaugų priklausomybė nuo informacinių sistemų, tarpsisteminių sąsajų sudėtingumas, trečiųjų šalių dalyvavimas bei organizacijų pasirengimas valdyti sutrikimus. Didžiausia rizika kyla tais atvejais, kai

duomenų konfidencialumo, vientisumo ar prieinamumo pažeidimai kartu paveikia paslaugų tęstinumą, todėl incidentų valdymas turi būti siejamas su veiklos kritiškumo vertinimu ir organizacinio atsparumo užtikrinimu.

2.2. Sisteminė incidentų ir atakų analizė parodė, kad e. sveikatos sistemos kibernetinis atsparumas priklauso nuo organizacijos gebėjimo nuosekliai vykdyti visą incidentų valdymo ciklą – nuo grėsmių identifikavimo ir reagavimo iki veiklos atkūrimo bei poįvykiminės analizės. Tyrimo rezultatai išryškino, kad būtent incidentų valdymo tęstinumas ir grįžtamojo ryšio integravimas į vadybinius sprendimus yra reikšmingi veiksniai, siejant operacinį reagavimą su ilgalaikiu organizaciniu pasirengimu.

2.3. Sisteminė incidentų ir atakų analizė atskleidė, kad e. sveikatos kibernetinis atsparumas priklauso nuo tarpusavyje susietų vadybinių ir organizacinių mechanizmų – rizikų valdymo, prieigos kontrolės, duomenų apsaugos, tiekėjų priežiūros, darbuotojų kompetencijų stiprinimo ir organizacinio mokymosi po incidentų. Šių mechanizmų integravimas į bendrą valdymo sistemą sudaro pagrindą nuosekliau valdyti ne tik pavienes grėsmes, bet ir jų galimą sisteminį poveikį e. sveikatos paslaugų tęstinumui.

3. Teorinės analizės ir e. sveikatos sistemos valdymo ypatumų pagrindu suformuotas koncepcinis kibernetinio saugumo valdymo modelis, integruojantis strateginį, taktinį, operacinį ir technologinį valdymo lygmenis. Modelio struktūra sudaro pagrindą nuosekliai susieti atsakomybių paskirstymą, rizikų ir incidentų valdymą, informacijos srautų kontrolę bei kibernetinio saugumo brandos vertinimą.

3.1. Koncepcinio modelio struktūroje išskirti strateginis, taktinis, operacinis ir technologinis valdymo lygmenys sudaro sąlygas kibernetinio saugumo sprendimus vertinti kaip tarpusavyje susijusią vadybinių veiksmų sistemą. Toks struktūravimas leidžia aiškiau atskirti sprendimų priėmimo, jų įgyvendinimo ir kontrolės atsakomybes bei susieti jas su skirtingais e. sveikatos sistemos valdymo lygmenimis.

3.2. Koncepcinio modelio struktūra pagrįsta tarpusavyje susietomis vadybinėmis ir funkcinėmis dimensijomis – atsakomybių paskirstymu, rizikų ir incidentų valdymu, informacijos srautų kontrole, duomenų apsauga, teisine atitiktimi, brandos vertinimu ir nuolatiniu tobulinimu. Šių dimensijų integravimas į strateginį, taktinį, operacinį ir technologinį valdymo lygmenis sudaro pagrindą nuosekliai koordinuoti sprendimų priėmimą, atsakomybę ir kontrolės priemonių įgyvendinimą visame e. sveikatos sistemos valdymo cikle.

3.3. Parengtas koncepcinis modelis suformavo analitinį pagrindą empiriškai vertinti e. sveikatos kibernetinio saugumo valdymo spragas ir nustatyti, kurie vadybiniai mechanizmai turi būti stiprinami praktiniame modelio taikyme. Ekspertinio tyrimo rezultatai leido patikslinti modelio struktūrą, išryškinant atsakomybių paskirstymo, valdymo lygmenų koordinavimo,

rizikomis grindžiamo sprendimų priėmimo ir organizacinio mokymosi reikšmę.

4. Ekspertinio tyrimo rezultatai atskleidė, kad e. sveikatos organizacijų kibernetinio saugumo valdymo ribotumai pirmiausia siejami su valdymo fragmentacija, nepakankamai aiškiu atsakomybių paskirstymu ir silpna skirtingų valdymo lygmenų sąveika. Šių problemų sprendimui būtinas nuoseklesnis rizikų ir incidentų valdymo integravimas į organizacijos sprendimų priėmimo procesus, aiškesnis koordinavimas ir sisteminis organizacinis mokymasis.
    4.1. Ekspertinių interviu rezultatai parodė, kad e. sveikatos organizacijose kibernetinio saugumo valdymo trūkumai pirmiausia siejami su nepakankamu jo integravimu į bendrą organizacijos valdymą. Ekspertų vertinimu, neaiškiai paskirstytos atsakomybės, ribotas vadovybės įsitraukimas ir nepakankamas tarpinstitucinis koordinavimas silpnina galimybes nuosekliai įgyvendinti kibernetinio saugumo reikalavimus praktikoje.
    4.2. TK1–TK4 analizė parodė, kad pagrindinės e. sveikatos kibernetinio saugumo valdymo problemos kyla ne dėl pavienių techninių trūkumų, bet dėl nepakankamo valdymo procesų tarpusavio susiejimo. Ekspertų vertinimu, didžiausią reikšmę turi aiškus atsakomybių paskirstymas, strateginio, taktinio, operacinio ir technologinio valdymo lygmenų koordinavimas bei nuoseklus rizikų ir incidentų valdymas. Šie rezultatai sudarė empirinį pagrindą modelį tikslinti stiprinant jo vadybinius mechanizmus.
    4.3. Atsižvelgiant į ekspertų identifikuotas problemas ir empirinio tyrimo rezultatus, koncepcinis modelis buvo patikslintas, daugiau dėmesio skiriant vadybiniams jo įgyvendinimo mechanizmams. Modelyje sustiprinti atsakomybių paskirstymo, padalinių ir institucijų koordinavimo, rizikomis grindžiamo išteklių planavimo, incidentų valdymo, grįžtamojo ryšio ir brandos vertinimo elementai. Šie papildymai leidžia modelį glaudžiau susieti su praktiniais e. sveikatos organizacijų valdymo procesais ir ekspertų nustatytomis problemomis.
5. Ekspertinis patikslinto kibernetinio saugumo valdymo modelio vertinimas parodė, kad jo struktūra yra logiškai nuosekli, atitinka ekspertų identifikuotus e. sveikatos kibernetinio saugumo valdymo poreikius ir gali būti taikoma kaip praktinis pagrindas valdymo spragoms nustatyti bei tobulinimo prioritetams formuoti.
    5.1. Ekspertinių interviu rezultatai sudarė pagrindą įvertinti siūlomo modelio praktinę reikšmę e. sveikatos organizacijų kibernetinio saugumo valdymui. Ekspertai modelio taikymo galimybes siejo su aiškesniu atsakomybių paskirstymu, rizikomis grindžiamu išteklių planavimu, nuoseklesniu rizikų ir incidentų valdymu, tarpinstitucinio koordinavimo stiprinimu bei kryptingesniu kibernetinio saugumo brandos didinimu.
    5.2. Ekspertų vertinimu, didžiausią praktinę reikšmę turi modelyje numatytas aiškesnis atsakomybių paskirstymas, incidentų valdymo struktūrizavimas ir valdymo sprendimų pritaikymas e. sveikatos sistemos specifikai.

Šie elementai sudaro vadybinį pagrindą nuosekliau organizuoti kibernetinio saugumo procesus ir mažinti ekspertų identifikuotą atotrūkį tarp formalių reikalavimų ir jų praktinio įgyvendinimo.

5.3. Kendall konkordacijos koeficientas parodė aukštą ekspertų vertinimų suderinamumą, todėl gauti rezultatai laikytini nuosekliais tyrimo imties ribose. Ekspertinis vertinimas pagrindė patikslinto modelio tinkamumą valdymo fragmentiškumui identifikuoti, atsakomybių aiškumui stiprinti ir rizikų bei incidentų valdymo sąsajoms struktūruoti.

6. Teorinės ir empirinės analizės rezultatai leido suformuluoti patikslinto kibernetinio saugumo valdymo modelio taikymo rekomendacijas, orientuotas į vadybinių sprendimų nuoseklumą, atsakomybių paskirstymą, rizikomis grindžiamą išteklių planavimą, tarpinstitucinį koordinavimą ir periodinį kibernetinio saugumo brandos vertinimą. Šių mechanizmų integravimas sudaro praktinį pagrindą sistemiškai taikyti modelį e. sveikatos organizacijų valdymo procesuose.

6.1. Patikslinto modelio taikymas grindžiamas jo integravimu į pagrindinius organizacijos valdymo procesus – strateginį planavimą, atsakomybių paskirstymą, rizikų ir incidentų valdymą, išteklių planavimą bei veiklos rezultatų stebėseną. Toks taikymo principas leidžia modelį naudoti ne tik kibernetinio saugumo būklei aprašyti, bet ir kaip vadybinį instrumentą valdymo spragoms nustatyti, prioritetams pagrįsti ir organizacijos brandos pokyčiams vertinti.

6.2. Parengtos rekomendacijos operacionalizuoja patikslinto modelio taikymą, susiedamos jo struktūrinius elementus su konkrečiais vadybiniais veiksmais: valdymo būklės vertinimu, prioritetų nustatymu, atsakomybių paskirstymu, rizikų ir incidentų valdymo integravimu bei technologinių sprendimų derinimu su organizacijos valdymo tikslais. Toks taikymo principas sudaro prielaidas nuosekliau vertinti kibernetinio saugumo brandą ir kryptingai planuoti jos tobulinimą.

6.3. Praktinio taikymo gairės papildo patikslintą modelį konkrečiais jo įgyvendinimo mechanizmais ir sudaro sąlygas modelį taikyti kaip nuoseklaus kibernetinio saugumo valdymo tobulinimo pagrindą. Modelio taikymo rezultatai turėtų būti vertinami periodiškai, analizuojant brandos pokyčius, incidentų valdymo rodiklius, veiklos tęstinumo būklę ir kitus organizacijos parengtį atspindinčius kriterijus. Toks vertinimas leistų pagrįstai nustatyti, kokiu mastu modelio taikymas siejasi su kibernetinio saugumo valdymo pažanga konkrečios e. sveikatos organizacijos kontekste.

REKOMENDACIJOS

• *Patikslintą kibernetinio saugumo valdymo modelį e. sveikatos sistemos tobulinimui taikyti kaip strateginį e. sveikatos sistemos kibernetinio saugumo valdymo pagrindą.*

Rekomenduojama patikslintą modelį naudoti kaip orientacinę valdymo struktūrą, padedančią e. sveikatos sistemos kibernetinį saugumą susieti su strateginiais sveikatos sektoriaus skaitmenizavimo, paslaugų tęstinumo, pacientų saugos ir kritinės infrastruktūros apsaugos tikslais. Modelis turėtų būti integruojamas į nacionalinio ir organizacinio lygmens strateginius dokumentus, kibernetinio saugumo politikas, informacijos saugumo valdymo sistemas ir e. sveikatos plėtros programas.

Taikant modelį, kibernetinis saugumas neturėtų būti suprantamas kaip atskira techninė funkcija. Jis turėtų būti vertinamas kaip integruota valdymo sritis, kurioje strateginiai sprendimai, organizacinės atsakomybės, rizikų valdymas, incidentų valdymas, technologinės priemonės ir teisinė atitiktis veikia kaip tarpusavyje susiję elementai.

• *Modelį naudoti kaip diagnostinę priemonę kibernetinio saugumo valdymo spragoms nustatyti.*

Rekomenduojama patikslintą modelį taikyti atliekant e. sveikatos organizacijų kibernetinio saugumo valdymo būklės vertinimą. Vertinimas turėtų apimti modelyje išskirtus valdymo lygmenis – strateginį, taktinį, operacinį ir technologinį – bei funkcines dimensijas: rizikų valdymą, incidentų valdymą, atsakomybių paskirstymą, informacijos srautų saugumą, duomenų apsaugą, teisinę atitiktį, brandos vertinimą ir nuolatinį tobulinimą.

Praktikoje tai galėtų būti įgyvendinama kaip periodinis savęs vertinimas arba vidaus audito priemonė. Kiekviena organizacija, taikydama modelį, turėtų įvertinti, kurie modelio elementai jau yra įgyvendinti, kurie veikia fragmentiškai, o kurių trūksta. Tokiu būdu modelis leistų ne tik aprašyti esamą situaciją, bet ir nustatyti prioritetines tobulinimo kryptis, susijusias su atsakomybių aiškumu, rizikų valdymo integracija, incidentų valdymo pasirengimu, technologinių priemonių pakankamumu ir organizaciniu mokymusi.

• *Modelio pagrindu aiškiai paskirstyti atsakomybes tarp strateginio, taktinio, operacinio ir technologinio valdymo lygmenų.*

Empirinio tyrimo rezultatai parodė, kad viena iš svarbiausių e. sveikatos kibernetinio saugumo valdymo problemų yra atsakomybių neapibrėžtumas ir valdymo fragmentiškumas. Todėl rekomenduojama modelį naudoti kaip atsakomybių paskirstymo pagrindą. Strateginiame lygmenyje turėtų būti apibrėžta vadovybės atsakomybė už kibernetinio saugumo prioritetus, rizikos toleranciją, išteklių skyrimą ir saugumo rodiklių vertinimą. Taktiniame lygmenyje turėtų būti nustatytos koordinavimo funkcijos, politikų ir procedūrų rengimas, padalinių bendradarbiavimo mechanizmai. Operaciniame lygmenyje turėtų būti apibrėžti kasdieniai saugumo procesai, incidentų registravimas, reagavimas, eskalavimas ir atkūrimas. Technologiniame lygmenyje turėtų

būti numatytos konkrečios kontrolės priemonės, susijusios su prieigos valdymu, stebėsena, infrastruktūros apsauga ir duomenų saugumu. Tokiu būdu modelis galėtų būti taikomas kaip praktinė priemonė atsakomybių matricai sudaryti.

• *Kibernetinio saugumo išteklių paskirstymą grįsti rizikų vertinimu ir nustatytais valdymo prioritetais.*

Rekomenduojama sprendimus dėl finansinių, žmogiškųjų ir technologinių išteklių skyrimo kibernetiniam saugumui tiesiogiai sieti su organizacijos rizikų vertinimo rezultatais, kritinių e. sveikatos paslaugų reikšmingumu ir nustatytomis valdymo spragomis. Tokiu būdu išteklių paskirstymas būtų grindžiamas ne pavieniais technologiniais poreikiais ar reaktyviu reagavimu į incidentus, bet nuosekliu organizacijos kibernetinio saugumo prioritetų vertinimu.

Taikant patikslintą modelį, aukščiausio lygmens vadovybė turėtų periodiškai vertinti, ar turimi ištekliai atitinka nustatytą rizikos lygį ir pasirinktus kibernetinio saugumo tikslus. Tai sudarytų prielaidas kryptingiau planuoti investicijas, darbuotojų kompetencijų stiprinimą, technologinių priemonių diegimą ir veiklos tęstinumui reikalingus sprendimus.

• *Stiprinti tarpinstitucinį kibernetinio saugumo valdymo koordinavimą e. sveikatos sistemoje.*

E. sveikatos sistemos kibernetinis saugumas priklauso nuo skirtingų institucijų, sveikatos priežiūros įstaigų, informacinių sistemų valdytojų ir technologinių paslaugų teikėjų tarpusavio sąveikos. Todėl rekomenduojama aiškiai apibrėžti tarpinstitucinio koordinavimo tvarką, atsakomybes, informacijos apsikeitimo principus ir veiksmus kibernetinių incidentų metu.

Praktikoje tai gali būti įgyvendinama nustatant nuolatinius koordinavimo mechanizmus, bendrus kontaktinius taškus, suderintas incidentų eskalavimo procedūras ir periodines bendras pratybas. Tokia sąveika sudarytų prielaidas greičiau keistis informacija apie rizikas ir incidentus, sumažintų atsakomybių dubliavimąsi ir padėtų nuosekliau įgyvendinti kibernetinio saugumo reikalavimus visoje e. sveikatos sistemoje.

• *Modelio pagrindu integruoti rizikų ir incidentų valdymą į vieną nuoseklų ciklą.*

Rekomenduojama modelį taikyti siekiant susieti rizikų valdymą, incidentų valdymą ir organizacinį mokymąsi. Rizikų vertinimas neturėtų apsiriboti formaliu rizikų dokumentavimu. Jis turėtų būti naudojamas priimant sprendimus dėl saugumo priemonių prioritetų, finansavimo, infrastruktūros atnaujinimo, prieigos kontrolės, darbuotojų mokymų ir incidentų valdymo pasirengimo.

Incidentų valdymo srityje modelis turėtų būti taikomas kaip procesinė schema, apimanti incidentų identifikavimą, registravimą, klasifikavimą, eskalavimą, reagavimą, komunikaciją, paslaugų atkūrimą ir analizę po incidento. Po kiekvieno reikšmingo incidento turėtų būti vertinama, kokie modelio elementai veikė tinkamai, o kurie reikalauja tobulinimo.

• *Patikslintą modelį taikyti technologinių saugumo priemonių planavimui ir prioritetų nustatymui.*

Rekomenduojama modelį naudoti ne tik vadybiniams, bet ir technologiniams sprendimams planuoti. Modelis turėtų padėti susieti technologines saugumo priemones su rizikų vertinimu, organizacijos brandos lygiu ir e. sveikatos sistemos veiklos kritiškumu. Planuojant technologines priemones, ypatingas dėmesys turėtų būti skiriamas tapatybės ir prieigos valdymui, naudotojų teisių kontrolei, privilegijuotų naudotojų priežiūrai, saugumo įvykių stebėsenai, žurnalinių įrašų analizei, duomenų apsaugai, atsarginių kopijų valdymui, medicininių įrenginių saugumui ir tarpsisteminių integracijų apsaugai.

Modelis taip pat turėtų būti naudojamas vertinant, ar technologiniai sprendimai nėra diegiami fragmentiškai. Technologinės investicijos turėtų būti pagrįstos ne vien techniniu poreikiu, bet ir jų poveikiu visai kibernetinio saugumo valdymo sistemai. Tai leistų užtikrinti, kad technologinis lygmuo būtų susietas su strateginiais ir taktiniais sprendimais, o saugumo priemonės būtų planuojamos ne pavieniui, bet kaip vientisos saugumo architektūros dalis.

• *Modelį integruoti į e. sveikatos sistemos tobulinimo ir projektų valdymo procesus.*

Kadangi modelis orientuotas į e. sveikatos sistemos projektavimo, diegimo, administravimo ir tobulinimo etapus, rekomenduojama jį taikyti ne tik eksploatuojamų sistemų saugumo vertinimui, bet ir naujų e. sveikatos sprendimų planavimui. Kiekviename e. sveikatos sistemos plėtros ar modernizavimo projekte modelio elementai turėtų būti naudojami kaip kontroliniai klausimai: ar nustatytos atsakomybės, ar atliktas rizikų vertinimas, ar numatyti incidentų valdymo veiksmai, ar užtikrintas informacijos srautų saugumas, ar numatytas sistemos stebėsenos ir tobulinimo mechanizmas.

Toks modelio taikymas leistų kibernetinį saugumą integruoti ne po sistemos įdiegimo, bet nuo ankstyvųjų projektavimo ir diegimo etapų. Tai ypač svarbu e. sveikatos sistemoje, kur nauji sprendimai dažnai susiję su jautrių sveikatos duomenų tvarkymu, skirtingų informacinių sistemų sąveika ir paslaugų prieinamumo reikalavimais.

LITERATŪRA

1. Aakanksha, T., Krishna, B. C. (2025). Security and cybersecurity risk management in e-health systems: A hybrid approach. International Journal of Safety and Security Engineering, 15(8), 1603–1610. https://doi.org/10.18280/ijsse.150806
2. Abomhara, M., ir Køien, G. M. (2015). Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), 65–88. https://doi.org/10.13052/jcsm2245-1439.414
3. Abunadi, I., ir Kumar, R. L. (2021). BSF-EHR: Blockchain Security Framework for Electronic Health Records of Patients. Sensors, 21(8), 2865. https://doi.org/10.3390/s21082865
4. Adler-Milstein, J., Everson, J., ir Lee, S. D. (2015). EHR adoption and hospital performance: Time-related effects. Health Services Research, 50(6), 1751–1771. https://doi.org/10.1111/1475-6773.12406
5. Ahmad, A., Maynard, S. B., ir Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. Journal of Intelligent Manufacturing, 30(1), 397–410. https://doi.org/10.1007/s10845-012-0683-0
6. Ahmad, A., Maynard, S. B., ir Shanks, G. (2015). A case analysis of information systems and security incident responses. International Journal of Information Management, 35(6), 717–723. https://doi.org/10.1016/j.ijinfomgt.2015.08.001
7. Alanazi, A. T. (2023). Clinicians' perspectives on healthcare cybersecurity and cyber threats. Cureus, 15(10), Article e47026. https://doi.org/10.7759/cureus.47026
8. Aldosari, B. (2025). Cybersecurity in healthcare: New threat to patient safety. Cureus, 17(5), Article e83614. https://doi.org/10.7759/cureus.83614
9. Alharbi, A., ir Alkhalifah, A. (2025). Cybersecurity governance in the healthcare sector during digital transformation: An integrated model and hybrid analytical approach. Frontiers in Public Health, 13, 1703689. https://doi.org/10.3389/fpubh.2025.1703689
10. Al-Momani, A. M., Ramayah, T., ir Al-Sharafi, M. A. (2024). Exploring the impact of cybersecurity on using electronic health records and their performance among healthcare professionals: A multi-analytical SEM-ANN approach. Technology in Society, 77, Article 102592. https://doi.org/10.1016/j.techsoc.2024.102592
11. Alhuwail, D., Al-Jafar, E., Abdulsalam, Y., ir AlDuaij, S. (2021). Information security awareness and behaviors of health care professionals at public health care facilities. Applied Clinical Informatics, 12(4), 924–932. https://doi.org/10.1055/s-0041-1735527
12. Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers and Security, 98, 102003. https://doi.org/10.1016/j.cose.2020.102003
13. Alsubaei, F., Abuhussein, A., ir Shiva, S. (2017). Security and privacy in the Internet of Medical Things: Taxonomy and risk assessment. In 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), 112–120, IEEE. https://doi.org/10.1109/LCN.Workshops.2017.72
14. Amato, F., Casola, V., Cozzolino, G., De Benedictis, A., Mazzocca, N., ir Moscato, F. (2021). A security and privacy validation methodology for e-health systems. ACM

Transactions on Multimedia Computing, Communications, and Applications, 17(2s), Article 67. https://doi.org/10.1145/3412373
15. Anderson, R. (2020). Security engineering: A guide to building dependable distributed systems (3rd ed.). Wiley.
16. Anderson, R., ir Moore, T. (2006). The economics of information security. Science, 314(5799), 610-613. https://doi.org/10.1126/science.1130992
17. Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., ir Savage, S. (2019). Measuring the cost of cybercrime. Journal of Cybersecurity, 5(1), 1-21. https://doi.org/10.1007/978-3-642-39498-0_12
18. Appari, A., ir Johnson, M. E. (2010). Information security and privacy in healthcare: Current state of research. International Journal of Internet and Enterprise Management, 6(4), 279-314. https://doi.org/10.1504/IJIEM.2010.035624
19. Ashby, W. R. (1956). An introduction to cybernetics. Chapman and Hall.
20. Ashenden, D., ir Lawrence, D. (2016). Can we sell security like soap? A new approach to behaviour change. Computer Fraud and Security, 2016(1), 17-20. https://doi.org/10.1145/2535813.2535823
21. Augustinaitis A.; Rudzkienė V.; Petrauskas R. A.; Dagytė I.; Martynaitytė E.; Leich teris E.; Malinauskienė E.; Višnevska V.; Žilionienė I., 2009. Lietuvos e. valdžios gairės: ateities įžvalgų tyrimas, kolektyvinė monografija, Mykolo Romerio univer sitetas, ISBN 9789955191605. https://www.lituanistika.lt/content/24041?
22. Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research, 253(1), 1-13. https://doi.org/10.1016/j.ejor.2015.12.023
23. Bada M, Nurse JR (2019), Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Information and Computer Security, Vol. 27 No. 3 pp. 393–410, doi: https://doi.org/10.1108/ICS-07-2018-0080
24. Bada, M., ir Nurse, J. R. C. (2020). The social and psychological impact of cyberattacks. In V. Benson ir J. McAlaney (Eds.), Emerging Cyber Threats and Cognitive Vulnerabilities (pp. 73–92). Academic Press. https://doi.org/10.1016/B978-0-12-816203-3.00004-6
25. Bada, M., Sasse, A. M., ir Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? Cybersecurity, 2(1), 1-17. https://doi.org/10.48550/arXiv.1901.02672
26. Bamberger, K. A., ir Mulligan, D. K. (2011). Privacy on the books and on the ground. Stanford Law Review, 63(2), 247-315.
27. Baskerville, R., Spagnoletti, P., ir Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. Information and Management, 51(1), 138-151. https://doi.org/10.1016/j.im.2013.11.004
28. Singer, P. W., ir Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press. https://doi.org/10.1093/wentk/9780199918096.001.0001

29. Benson, T., ir Grieve, G. (2016). Principles of health interoperability: SNOMED CT, HL7 and FHIR (2nd ed.). Springer. https://doi.org/10.1007/978-3-319-30370-3
30. Bente, B. E., van Dongen, A., Verdaasdonk, R., ir van Gemert-Pijnen, L. (2024). eHealth implementation in Europe: A scoping review on legal, ethical, financial, and technological aspects. Frontiers in Digital Health, 6, 1332707. https://doi.org/10.3389/fdgth.2024.1332707
31. Bialas, A. (2016). Risk Management in Critical Infrastructure — Foundation for Its Sustainable Work. Sustainability, 8(3), 240. https://doi.org/10.3390/su8030240
32. Braun, V., ir Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
33. Brantly, N. D. (2026). The U.S. health system vulnerabilities. BMC Health Services Research, 26, Article 32. https://doi.org/10.1186/s12913-025-13803-5
34. Bodeau, D. J., ir Graubart, R. (2017). Cyber resiliency design principles. MIT Lincoln Laboratory Technical Report.
35. Boehm, B. W. (1984). Verifying and validating software requirements and design specifications. IEEE Software, 1(1), 75-88. https://doi.org/10.1109/MS.1984.233702
36. Botsis, T., Hartvigsen, G., Chen, F., ir Weng, C. (2010). Secondary use of EHR: Data quality issues and informatics opportunities. Studies in Health Technology and Informatics, 160, 1-5. PMID: 21347133; PMCID: PMC3041534.
37. Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27-40. https://doi.org/10.3316/QRJ0902027
38. Boyes, H., Hallaq, B., Cunningham, J., ir Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. Computers in Industry, 101, 1–12. https://doi.org/10.1016/j.compind.2018.04.015
39. Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation, 34(7), 342-353. https://doi.org/10.1016/j.technovation.2014.02.001
40. Bohme, R., Laube, S., ir Riek, M. (2021). Cybersecurity maturity and its measurement. Journal of Cybersecurity, 8(1), 1-14.
41. Bracciale, L., Loreti, P., ir Bianchi, G. (2023). Cybersecurity vulnerability analysis of medical devices purchased by national health services. Scientific Reports, 13, 19509. https://doi.org/10.1038/s41598-023-45927-1
42. Braun, V., ir Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
43. Bromiley, P., McShane, M., Nair, A., ir Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. Long Range Planning, 48(4), 265-276. https://doi.org/10.1016/j.lrp.2014.07.005
44. Bulgurcu, B., Cavusoglu, H., ir Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523-548.
45. Burke, W., Stranieri, A., Oseni, T. (2025). From dis-empowerment to empowerment: Crafting a healthcare cybersecurity self-assessment. Computers and Security, 148, Article 104148. https://doi.org/10.1016/j.cose.2024.104148

46. Burke, W., Stranieri, A., Oseni, T., Gondal, I. (2024). The need for cybersecurity self-evaluation in healthcare. BMC Medical Informatics and Decision Making, 24, Article 133. https://doi.org/10.1186/s12911-024-02551-x
47. Camara, C., Peris-Lopez, P., ir Tapiador, J. E. (2015). Security and privacy issues in implantable medical devices: A comprehensive survey. Journal of Biomedical Informatics, 126, 103997.
48. Cambridge Dictionary. (n.d.). Model. Cambridge University Press. https://dictionary.cambridge.org/dictionary/english/model
49. Caralli, R. A., Knight, M., ir Montgomery, A. (2012). Maturity models for cyber resilience. IEEE Security and Privacy, 10(1), 70-73.
50. Cavoukian, A. (2011). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario.
51. Casanova, R., Villa-Garzon, F. A., ir Branch-Bedoya, J. W. (2025). Architectural patterns for health information systems: A systematic review. Frontiers in Digital Health, 7, 1694839. https://doi.org/10.3389/fdgth.2025.1694839
52. Cichonski, P., Millar, T., Grance, T., ir Scarfone, K. (2018). Computer security incident handling guide (NIST SP 800-61 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2
53. Clarke, M., Martin, K. (2024). Managing cybersecurity risk in healthcare settings. Healthcare Management Forum, 37(1), 17–20. https://doi.org/10.1177/08404704231195804
54. Cornejo, G. M. (2026). Third-party risk in U.S. health care ransomware incidents: Business associate involvement and breach size. Health and Technology, 16, 609–620. https://doi.org/10.1007/s12553-025-01036-9
55. Coutinho, B., Ferreira, J., Yevseyeva, I., ir Basto-Fernandes, V. (2023). Integrated cybersecurity methodology and supporting tools for healthcare operational information systems. Computers and Security, 129, Article 103189. https://doi.org/10.1016/j.cose.2023.103189
56. Coiera, E., Aarts, J., ir Kulikowski, C. (2012). The dangerous decade. Journal of the American Medical Informatics Association, 25(1), 130-132. https://doi.org/10.1136/amiajnl-2011-000674
57. Coventry, L., ir Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48-52. https://doi.org/10.1016/j.maturitas.2018.04.008
58. Craigen, D., Diakun-Thibault, N., ir Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10), 13-21.
59. Cresswell, K. M., ir Sheikh, A. (2013). Organizational issues in the implementation and adoption of health information technology innovations: An interpretative review. International Journal of Medical Informatics, 82(5), e73-e86. https://doi.org/10.1016/j.ijmedinf.2012.10.007
60. Culot, G., Fattori, F., Podrecca, M., ir Sartor, M. (2021). Addressing Industry 4.0 cybersecurity challenges. Computers in Industry, 129, 103433.
61. Da Veiga, A., ir Eloff, J. H. P. (2007). An information security

governance framework. Information Systems Management, 34(4), 361-372. https://doi.org/10.1080/10580530701586136
62. Dameff, C., Tully, J., Chan, T. C., Castillo, E. M., Savage, S., Maysent, P., Hemmen, T. M., Clay, B. J., ir Longhurst, C. A. (2023). Ransomware attack associated with disruptions at adjacent emergency departments in the US. JAMA Network Open, 6(5), e2312270. https://doi.org/10.1001/jamanetworkopen.2023.12270
63. De Bruijn, H., ir Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based maturity models. Government Information Quarterly, 34(1), 1-10. https://doi.org/10.1016/j.giq.2017.02.007
64. Di Palma, G., Scendoni, R., Ferorelli, D., De Benedictis, A., Tambone, V., De Micco, F. (2025). AI-induced cybersecurity risks in healthcare: A narrative review of blockchain-based solutions within a clinical risk management framework. Risk Management and Healthcare Policy, 18, 3479–3497. https://doi.org/10.2147/RMHP.S544523
65. De Haes, S., ir Van Grembergen, W. (2015). Enterprise governance of information technology: Achieving strategic alignment and value. Springer. https://doi.org/10.1007/978-0-387-84882-2
66. De Hert, P., ir Papakonstantinou, V. (2021). The GDPR as a cybersecurity regulation. Computer Law and Security Review, 40, 105518. https://doi.org/10.1016/j.clsr.2016.02.006
67. Dekker, S. (2017). Just culture: Restoring trust and accountability in your organization (3rd ed.). CRC Press. https://doi.org/10.1201/9781315590813
68. Dhillon, G. (2007). Principles of information systems security: Texts and cases. John Wiley and Sons.
69. Dhillon, G., ir Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. Information Systems Journal, 11(2), 127-153. https://doi.org/10.1046/j.1365-2575.2001.00099.x
70. Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security, 4(2), 92-100. https://doi.org/10.4236/jis.2013.42011
71. Dupont, B., Shearing, C., Bernier, M., ir Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. Computers and Security, 132, 103372. https://doi.org/10.1016/j.cose.2023.103372
72. Eysenbach, G. (2001). What is e-health? Journal of Medical Internet Research, 3(2), e20. https://doi.org/10.2196/jmir.3.2.e20
73. ENISA. (2021). Threat landscape for healthcare sector. European Union Agency for Cybersecurity.
74. ENISA. (2022). Cybersecurity maturity assessment frameworks. European Union Agency for Cybersecurity.
75. ENISA. (2022). Threat landscape for health sector. European Union Agency for Cybersecurity.
76. ENISA. (2023). Cybersecurity resilience for healthcare. European Union Agency for Cybersecurity.

77. ENISA. (2023). NIS2 Directive: Technical implementation guidance. European Union Agency for Cybersecurity.
78. Europos Komisijos dirbtinio intelekto kalbos įrankiai vertimui. AI translation and language tools - Multilingualism, translation and language-based AI services
79. Europos Parlamentas ir Taryba (2016). Regulation (EU) 2016/679 (General Data Protection Regulation) (BDAR)
80. Europos Parlamentas ir Taryba. (2022). Direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti (TIS2, angl. NIS2).
81. Ewoh, P., Vartiainen, T. (2024). Vulnerability to cyberattacks and sociotechnical solutions for health care systems: Systematic review. Journal of Medical Internet Research, 26, e46904. https://doi.org/10.2196/46904
82. Ewoh, P., Vartiainen, T., Mantere, T. (2025). Sociotechnical cybersecurity framework for securing health care from vulnerabilities and cyberattacks: Scoping review. Journal of Medical Internet Research, 27, e75584. https://doi.org/10.2196/75584
83. Fernandez-Aleman, J. L., Señor, I. C., Lozoya, P. A. O., ir Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics, 46(3), 541-562. https://doi.org/10.1016/j.jbi.2012.12.003
84. Floridi, L., ir Taddeo, M. (2016). What is data ethics? Philosophical Transactions of the Royal Society A, 374(2083). https://doi.org/10.1098/rsta.2016.0360
85. Francis, R., Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliability Engineering ir System Safety, 121, 90–103. https://doi.org/10.1016/j.ress.2013.07.004
86. Freyer, O., Jahed, F., Ostermann, M., Rosenzweig, C., Werner, P., ir Gilbert, S. (2024). Consideration of cybersecurity risks in the benefit-risk analysis of medical devices: Scoping review. Journal of Medical Internet Research, 26, Article e65528. https://doi.org/10.2196/65528
87. Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martinez-Caro, E., ir Chinnaswamy, A. (2023). Resilience in healthcare systems: Cyber security and digital transformation. Technovation, 121, 102583. https://doi.org/10.1016/j.technovation.2022.102583
88. Gal-Or, E., ir Ghose, A. (2005). The economic incentives for sharing security information. Information Systems Research, 16(2), 186-208. https://doi.org/10.1287/isre.1050.0053
89. Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martinez-Caro, E., ir Chinnaswamy, A. (2023). Resilience in healthcare systems: Cyber security and digital transformation. Technovation, 121, 102583. https://doi.org/10.1016/j.technovation.2022.102583
90. Gordon, L. A., Loeb, M. P, and Zhou, L. (2016) Investing in Cybersecurity: Insights from the Gordon-Loeb Model. Journal of Information Security, 7, 49-59. https://doi.org/10.4236/jis.2016.72004.
91. Gordon, L. A., Loeb, M. P., ir Zhou, L. (2011). The impact of information security

breaches: Has there been a downward shift in costs? Journal of Computer Security, 29(1), 1-20. https://doi.org/10.3233/JCS-2009-0398
92. Gordon, L. A., Loeb, M. P., Lucyshyn, W., ir Zhou, L. (2021). Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb model. Journal of Information Security, 6, 24-30. https://doi.org/10.4236/jis.2015.61003.
93. Gordon, W. J., Fairhall, A., ir Landman, A. (2017). Threats to information security-public health implications. New England Journal of Medicine, 377, 707-709. https://doi.org/10.1056/NEJMp1707212
94. Greenhalgh, T., Wherton, J., Papoutsi, C., Lynch, J., Hughes, G., A'Court, C., Hinder, S., Fahy, N., Procter, R., ir Shaw, S. (2017). Beyond adoption: A new framework for theorizing and evaluating nonadoption, abandonment, and challenges to the scale-up of health and care technologies. Journal of Medical Internet Research, 19(11), e367. https://doi.org/doi:10.2196/jmir.8775
95. Gregor, S., ir Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. MIS Quarterly, 37(2), 337-355. https://doi.org/10.25300/MISQ/2013/37.2.01
96. Greitzer, F. L., Moore, A. P., Cappelli, D. M., Andrews, D. H., Carroll, L. A., ir Hull, T. D. (2014). Combating the insider cyber threat. IEEE Security and Privacy, 12(1), 61-64. https://doi.org/10.1109/MSP.2008.8.
97. Gurses, S., Troncoso, C., ir Diaz, C. (2021). Engineering privacy by design. Computer, 54(2), 38-48.
98. Guest, G., Bunce, A., ir Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. Field Methods, 18(1), 59–82. https://doi.org/10.1177/1525822X05279903
99. Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346
100. Hagen, J. M., Albrechtsen, E., ir Hovden, J. (2011). Implementation and effectiveness of organizational information security measures. Information Management ir Computer Security, 16(4), 377-397. https://doi.org/10.1108/09685220810908796
101. Halamka, J. D., Mandl, K. D., ir Tang, P. C. (2008). Early experiences with personal health records. Journal of the American Medical Informatics Association, 15(1), 1-7. https://doi.org/10.1197/jamia.M2562
102. Haleem, A., Javaid, M., Khan, I. H., ir Vaishya, R. (2021). Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 pandemic. Journal of Oral Biology and Craniofacial Research, 11(2), 209–214. https://doi.org/10.1016/j.jobcr.2021.01.015
103. Hasegawa, K., O'Brien, N., Prendergast, M., Ajah, C. A., Neves, A. L., ir Ghafur, S. (2024). Cybersecurity interventions in health care organizations in low- and middle-income countries: Scoping review. Journal of Medical Internet Research, 26, Article e47311. https://doi.org/10.2196/47311
104. Hayrinen, K., Saranto, K., ir Nykänen, P. (2008). Definition, structure, content, use

and impacts of electronic health records: A review of the research literature. International Journal of Medical Informatics, 77(5), 291-304. https://doi.org/10.1016/j.ijmedinf.2007.09.001
105. Herath, T., ir Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154-165. https://doi.org/10.1016/j.dss.2009.02.005
106. He, Y., Aliyu, A., Evans, M., ir Luo, C. (2021). Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. Journal of Medical Internet Research, 23(4), e21747. https://doi.org/10.2196/21747
107. Hevner, A. R., March, S. T., Park, J., ir Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75-105. https://doi.org/10.2307/25148625
108. Hochwarter, S. (2021). Sociotechnical challenges of eHealth technology for patient self-management: A systematic review. arXiv. https://doi.org/10.48550/arXiv.2102.07119
109. Hopkin, P. (2018). Fundamentals of risk management (4th ed.). Kogan Page.
110. Howard, J. D. (1997). An analysis of security incidents on the Internet 1989-1995. Carnegie Mellon University, Software Engineering Institute.
111. Hubbard, D. W., ir Seiersen, R. (2016). How to measure anything in cybersecurity risk. Wiley. https://doi.org/10.1002/9781119162315
112. OECD/European Union/EC-JRC (2008), Handbook on Constructing Composite Indicators: Methodology and User Guide, OECD Publishing, Paris, https://doi.org/10.1787/9789264043466-en.
113. O'Brien, N., Fernandez Crespo, R., O'Driscoll, F., Prendergast, M., Chana, D., Darzi, A., Ghafur, S. (2024). Usability and feasibility evaluation of a web-based and offline cybersecurity resource for health care organizations (The Essentials of Cybersecurity in Health Care Organizations Framework Resource): Mixed methods study. JMIR Formative Research, 8, Article e50968. https://doi.org/10.2196/50968
114. ISACA. (2019). COBIT 2019 framework: Governance and management objectives. ISACA.
115. ISO/IEC 27001:2022. Information security management systems - Requirements.
116. ISO/IEC 27002:2022. Information security controls.
117. ISO/IEC 27005:2018. Information technology - Security techniques - Information security risk management. International Organization for Standardization.
118. ISO/IEC 27005:2022. Information security risk management.
119. ISO/IEC 27035-1:2023. Information security incident management.
120. ISO/IEC 27701:2019. Privacy information management.
121. ISO/IEC. (2023). ISO/IEC 27032: Cybersecurity guidelines.
122. Ikegwu, A. C., Alo, U. R., Nweke, H. F., ir kt. (2025). Cyber threats in mobile healthcare applications: Systematic review of enabling technologies, threat models, detection approaches, and future directions. Discover Computing, 28(1), 1–45. https://doi.org/10.1007/s10791-025-09686-z
123. Iyengar, K. P., Jain, V. K., ir Vaishya, R. (2020). Current situation with doctors and

healthcare workers during COVID-19 pandemic in India. Postgraduate Medical Journal, 98(e2), e121–e122. https://doi.org/10.1136/postgradmedj-2020-138496
124. Jaidi, F., Ksibi, S., Bouhoula, A. (2025). An Internet of Medical Things cyber security assessment model (IoMT-CySAM). Cureus, 17(10), Article e94639. https://doi.org/10.7759/cureus.94639
125. Jalali, M. S., ir Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. Journal of Medical Internet Research, 20(5), e10059. https://doi.org/10.2196/10059
126. Jalali, M. S., Largman, K. (2025). Bridging data gaps and tackling human vulnerabilities in healthcare cybersecurity with generative AI. PLOS Digital Health, 4(10), Article e0001063. https://doi.org/10.1371/journal.pdig.0001063
127. Jansen, W., ir Grance, T. (2011). Guidelines on security and privacy in public cloud computing. IEEE Security and Privacy, 9(1), 44-51.
128. Jarvelainen, J. (2013). IT incidents and business impacts: Validating a framework for continuity management in information systems. International Journal of Information Management, 33(3), 583-590. https://doi.org/10.1016/j.ijinfomgt.2013.03.001
129. Kankanhalli, A., Teo, H. H., Tan, B. C. Y., ir Wei, K. K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management, 33(4), 584-593. https://doi.org/10.1016/S0268-4012(02)00105-6
130. Kardelis, K. (2019). Mokslinių tyrimų metodologija ir metodai. Vilnius: Mokslo ir enciklopedijų leidykla.
131. Katina, J.; Plėta, T.; Petkevičius, R.; Lelešienė, L. (2023). Industrial Control Systems (ICS) Cyber Prediction Model. Insights into Regional Development, 5(1), 86–96. https://doi.org/10.9770/IRD.2023.5.1(6)
132. Kellermann, A. L., ir Jones, S. S. (2013). What it will take to achieve the as-yet-unfulfilled promises of health information technology. Health Affairs, 32(1), 63-68. https://doi.org/10.1377/hlthaff.2012.0693
133. Khoumbati, K., Themistocleous, M., ir Irani, Z. (2006). Evaluating the adoption of enterprise application integration in health-care organizations. Journal of Management Information Systems, 22(4), 69–108. https://doi.org/10.2753/MIS0742-1222220404
134. Kjaerland, M. (2006). A taxonomy and comparison of computer security incidents from the commercial and government sectors. Computers and Security, 25(7), 522-538. https://doi.org/10.1016/j.cose.2006.08.004
135. Kohnke, A., Sigler, K., ir Shoemaker, D. (2016). The complete guide to cybersecurity risks and controls. CRC Press. https://doi.org/10.1201/b19631
136. Kruse, C. S., Frederick, B., Jacobson, T., ir Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review. JMIR Medical Informatics, 5(4), e45. https://doi.org/10.3233/THC-161263
137. Khallaf, F., El-Shafai, W., El-Rabaie, E.-S. M., ir Abd El-Samie, F. E. (2025). A systematic review of new technologies for cybersecurity healthcare applications: A systematic and comprehensive study. Transactions on Emerging Telecommunications Technologies, 36(7), Article e70183. https://doi.org/10.1002/ett.70183
138. Kissi, J., Adzakpah, G., Mensah, N. K., Dzamvivie, K., Bosompem, T. A., Wireko, V. A.,

Amoah-Anomah, G. (2024). Healthcare professionals' perception on emergence of security threat using digital health technologies in healthcare delivery. Digital Health, 10, Article 20552076241260385. https://doi.org/10.1177/20552076241260385
139. Ksibi, S., Jaidi, F., ir Bouhoula, A. (2022). A comprehensive study of security and cyber-security risk management within e-health systems: Synthesis, analysis and a novel quantified approach. Mobile Networks and Applications, 28, 107–127. https://doi.org/10.1007/s11036-022-02042-1
140. Ključnikov, A., Mura, L., ir Sklenár, D. (2019). Information security management in SMEs: Factors of success. Entrepreneurship and Sustainability Issues, 6(4), 2081–2094. https://doi.org/10.9770/jesi.2019.6.4(37)
141. Kvale, S., ir Brinkmann, S. (2015). InterViews: Learning the craft of qualitative research interviewing. SAGE Publications. ISBN 1452275726
142. Kwon, J., ir Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector. MIS Quarterly, 38(2), 451-471. https://doi.org/10.25300/MISQ/2014/38.2.06
143. Kwon, J., ir Johnson, M. E. (2014). Protecting patient data: Cybersecurity in healthcare. IEEE Security and Privacy, 12(6), 66-70. https://doi.org/10.1109/MSP.2015.113
144. Kwon, J., ir Johnson, M. E. (2013). Security practices and regulatory compliance in the healthcare industry. Journal of the American Medical Informatics Association, 20(1), 44–51 https://doi.org/10.1136/amiajnl-2012-000906
145. Lehne, M., Sass, J., Essenwanger, A., Schepers, J., ir Thun, S. (2019). Why digital medicine depends on interoperability. NPJ Digital Medicine, 2, 79. https://doi.org/10.1038/s41746-019-0158-1
146. Legendre, P. (2022). Coefficient of Concordance. In B. B. Frey (Ed.), The SAGE Encyclopedia of Research Design. SAGE Publications. https://doi.org/10.4135/9781071812082
147. Legendre, P. (2005). Species associations: The Kendall coefficient of concordance revisited. Journal of Agricultural, Biological, and Environmental Statistics, 10(2), 226–245. https://doi.org/10.1198/108571105X46642
148. Lieneck, C., Weaver, E., Maryon, T., ir Weaver, B. (2023). Healthcare cybersecurity ethical concerns during the COVID-19 global pandemic: A rapid review. Healthcare, 11(22), Article 2983. https://doi.org/10.3390/healthcare11222983
149. Lietuvos Respublikos valstybės kontrolė. (2008). Lietuvos Respublikos sveikatos apsaugos ministerijos informacinių sistemų bendrosios kontrolės vertinimas. Elektroninės sveikatos informacinės sistemos kūrimo auditas (Valstybinio audito ataskaita Nr. IA-9000-6-2).
150. Lietuvos Respublikos valstybės kontrolė. (2011). Elektroninės sveikatos informacinės sistemos plėtra ir audito rekomendacijų įgyvendinimas (Valstybinio audito ataskaita Nr. VA-P-90-2-10).
151. Lietuvos Respublikos valstybės kontrolė. (2017). Elektroninės sveikatos sistemos kūrimas (Valstybinio audito ataskaita, 2017 m. balandžio 26 d.).
152. Lietuvos Respublikos sveikatos apsaugos ministras. (2007). Dėl Lietuvos e.

sveikatos 2007–2015 metų plėtros strategijos patvirtinimo (2007 m. spalio 9 d. įsakymas Nr. V-811).
153. Lietuvos Respublikos sveikatos apsaugos ministras. (2010). Dėl E. sveikatos sistemos 2009–2015 metų plėtros programos patvirtinimo (2010 m. vasario 22 d. įsakymas Nr. V-151).
154. Lietuvos Respublikos sveikatos apsaugos ministras. (2018). Dėl Lietuvos e. sveikatos sistemos 2018–2025 metų plėtros programos įgyvendinimo priemonių plano patvirtinimo (2018 m. kovo 29 d. įsakymas Nr. V-362).
155. Lietuvos Respublikos sveikatos apsaugos ministras. (2019). Dėl Lietuvos e. sveikatos sistemos funkcinės, techninės ir programinės įrangos architektūros modelio patvirtinimo (2019 m. spalio 2 d. įsakymas Nr. V-1119).
156. Lietuvos Respublikos sveikatos apsaugos ministerija. (2024). Skaitmeninės sveikatos sistemos plėtros 2023–2027 metų veiksmų planas.
157. Lietuvos Respublikos Seimas. (2024). Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas (2024 m. liepos 11 d. Nr. XIV-2902). Teisės aktų registras, 2024-07-24, Nr. 2024-13535.
158. Limba, T., Plėta, T., Agafonov, K., ir Damkus, M. (2017). Cyber security management model for critical infrastructure. Entrepreneurship and Sustainability Issues, 4(4), 559-573. http://doi.org/10.9770/jesi.2017.4.4(12)
159. Limba, T.; Lelešienė, L.; Novogreckas, S.; Kowalewska, A. (2024). Harnessing Artificial Intelligence, Chatbots and Robots for Transformative Education: Exploring the Convergence. EDULEARN24: 16th International Conference on Education and New Learning Technologies, Palma, Spain, 1st–3rd of July, 2024. doi: 10.21125/edulearn.2024.1094
160. Limba, T.; Lelešienė, L.; Lelešius, V.; Novogreckas, S. (2025). Lessons from Large-Scale International Projects: Insights for Global Education, Collaboration, and AI Integration. EDULEARN25: 19th International Technology, Education and Development Conference, Valencia, Spain, 3rd–5th of March, 2025. doi: 10.21125/inted.2025.1639
161. Limba, T.; Lelešienė, L.; Novogreckas, S.; Kowalewska, A. (2023). Knowledge and Innovation Management. EDULEARN23: 15th International Conference on Education and New Learning Technologies, Palma, Spain, 3rd–5th of July, 2023. doi: 10.21125/edulearn.2023.0826
162. Linkov, I., ir Trump, B. D. (2019). The science and practice of resilience. Environment Systems and Decisions, 39(4), 417-421. https://doi.org/10.1007/978-3-030-04565-4
163. Linkov, I., Trump, B. D., Poinsatte-Jones, K., ir Florin, M. V. (2018). Governance strategies for a sustainable digital world. Sustainability, 11(16), 4405. https://doi.org/10.3390/su10020440
164. Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., ir Kott, A. (2013). Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), 471–476. https://doi.org/10.1007/s10669-013-9485-y
165. Malterud, K., Siersma, V. D., ir Guassora, A. D. (2016). Sample size in qualitative interview studies: Guided by information power. Qualitative Health Research, 26(13), 1753–1760. https://doi.org/10.1177/1049732315617444

166. Mandel, J. C., Kreda, D. A., Mandl, K. D., Kohane, I. S., ir Ramoni, R. B. (2016). SMART on FHIR: A standards-based, interoperable apps platform for electronic health records. Journal of the American Medical Informatics Association, 23(5), 899-908. https://doi.org/10.1093/jamia/ocv189
167. Europos Komisija. Multilingualism, translation and language-based AI services; AI translation and language tools https://translation.ec.europa.eu/tools-and-resources/ai-translation-and-language-tools_en
168. Clarke, M., ir Martin, K. (2024). Managing cybersecurity risk in healthcare settings. Healthcare Management Forum, 37(1), 17–20. https://doi.org/10.1177/08404704231195804
169. Martin, G., Martin, P., Hankin, C., Darzi, A., ir Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? BMJ, 358, j3179. https://doi.org/10.1136/bmj.j3179
170. Markopoulou, D., ir Papakonstantinou, V. (2021). The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges—The case of the health sector in particular. Computer Law and Security Review, 41, 105502. https://doi.org/10.1016/j.clsr.2020.105502
171. McLeod, A., ir Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. Decision Support Systems, 108, 57-68. https://doi.org/10.1016/j.dss.2018.02.007
172. Menon, V. M. V. (2026). Cybersecurity breaches in medical devices: Analyzing FDA safety communications in response to patient security concerns. Frontiers in Digital Health, 8, Article 1701551. https://doi.org/10.3389/fdgth.2026.1701551
173. Mikuletič, S., ir kt. (2024). Security and privacy oriented information security culture in healthcare: New dimensions and measurem
174. Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). Qualitative Data Analysis: A Methods Sourcebook (3rd ed.). SAGE Publications.ent. Computers and Security, 138, 103621. https://doi.org/10.1016/j.cose.2023.103489
175. Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. Nature Machine Intelligence, 1, 501-507. https://doi.org/10.1038/s42256-019-0114-4
176. Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos. (2025). Nacionalinė kibernetinio saugumo būklės ataskaita 2024.
177. NATO Cooperative Cyber Defence Centre of Excellence. (2022). Comparative study on the cyber defence of NATO member states. NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE).
178. Nguyen, O. T., Carey, A., Steege, L. M., ir Cho, H. (2026). Characteristics and contributors to workarounds in the electronic health record system among inpatient nurses: Secondary analysis of a mixed-methods study. International Journal of Nursing Studies, 173, 105261. https://doi.org/10.1016/j.ijnurstu.2025.105261
179. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., ir Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors, 21(15), 5119. https://doi.org/10.3390/s21155119
180. NIST. (2012). SP 800-61r2: Computer security incident handling guide.

181. NIST. (2014). Framework for improving critical infrastructure cybersecurity.
182. NIST. (2020). Cybersecurity Framework Profile for the Healthcare Sector. National Institute of Standards and Technology.
183. NIST. (2020). Framework for improving critical infrastructure cybersecurity (Version 1.1). National Institute of Standards and Technology.
184. NIST. (2023). NIST Cybersecurity Framework 2.0. National Institute of Standards and Technology.
185. Nacionalinis kibernetinio saugumo centras (NKSC). (2024). D.U.K. dėl Kibernetinio saugumo įstatymo ir Kibernetinio saugumo reikalavimų aprašo (KSRA): pereinamieji laikotarpiai, KSIS, KSS registras, CISO reikalavimai, tiekimo grandinės saugumas.
186. Nacionalinis kibernetinio saugumo centras (NKSC). (2024). ES projektai: nacionalinės SOC/CSIRT modulinės sistemos kūrimas TIS2 sektoriams ir 3 lygių (CSIRT-SOC-subjektai) apsaugos modelio plėtra.
187. Nacionalinis kibernetinio saugumo centras (NKSC). Įsigalioja atnaujintas Kibernetinio saugumo įstatymas: pagrindiniai pokyčiai ir įgyvendinimo etapai.
188. Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. Administration and Policy in Mental Health and Mental Health Services Research, 42, 533–544. https://doi.org/10.1007/s10488-013-0528-y
189. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., ir Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers and Security, 42, 165–176. https://doi.org/10.1016/j.cose.2013.12.003
190. Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., ir Jerram, C. (2015). The design of phishing studies: Challenges for researchers. Computers and Security, 52, 194–206. https://doi.org/10.1016/j.cose.2015.02.008
191. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., ir Jerram, C. (2017). The human aspects of information security questionnaire. Computers and Security, 65, 64-80. https://doi.org/10.1016/j.cose.2017.01.004
192. Paulk, M. C., Curtis, B., Chrissis, M. B., ir Weber, C. V. (1993). Capability maturity model for software. IEEE Software, 10(4), 18-27. https://doi.org/10.1109/52.219617
193. Pavao, J., Bastardo, R., ir Rocha, N. P. (2024). Cyber resilience and healthcare information systems: A systematic review. Procedia Computer Science, 239, 1255–1262. https://doi.org/10.1016/j.procs.2024.06.157
194. Patra, D., Rajagopalan, N. (2026). Integration of emerging technologies in cybersecurity for healthcare: A systematic review. Computers and Security, 161, Article 104763. https://doi.org/10.1016/j.cose.2025.104763
195. Piazza, A., ir Vasudevan, S. (2025). Mapping the cyberthreat landscape in healthcare using GDELT: A multimethod approach. Health Security, 23(3), 186–197. https://doi.org/10.1089/hs.2024.0016
196. Peffers, K., Tuunanen, T., Rothenberger, M. A., ir Chatterjee, S. (2007). A design

science research methodology for information systems research. Journal of Management Information Systems, 24(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302
197. Podrecca, M., Coluccia, A., ir Callegati, F. (2025). Systematic Review Cyber Risk Management: A Frameworks, Strategies, and Case Studies in Cybersecurity, 114, 102584. https://doi.org/10.13140/RG.2.2.17059.31523
198. Podsakoff P. M., Scott B. MacKenzie, Nathan P. Podsakoff. 2012. Sources of Method Bias in Social Science Research and Recommendations on How to Control It. Annual Review Psychology. 63:539-569. https://doi.org/10.1146/annurev-psych-120710-100452
199. Power, M. (2007). Organized uncertainty: Designing a world of risk management. Oxford University Press. https://doi.org/10.1093/oso/9780199253944.001.0001
200. Puhakainen, P., ir Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. MIS Quarterly, 34(4), 757-778. https://doi.org/10.2307/25750704
201. Qureshi, R., ir Koo, I. (2026). A comprehensive survey of cybersecurity threats and data privacy issues in healthcare systems. Applied Sciences, 16(3), Article 1511. https://doi.org/10.3390/app16031511
202. Radanliev, P., De Roure, D., ir Burnap, P. (2019). Cyber risk in IoT systems: A systematic review. Computers and Security, 112, 102510. https://doi.org/10.20944/preprints201903.0104.v1
203. Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Mantilla Montalvo, R., Cannady, S., ir Burnap, P. (2018). Future developments in cyber risk assessment for the Internet of Things. Computers in Industry, 102, 14–22 https://doi.org/10.1016/j.compind.2018.08.002
204. Rahmani, A.-M., Thanigaivelan, N. K., Gia, T. N., Granados, J., Negash, B., Liljeberg, P., ir Tenhunen, H. (2015). Smart e-Health gateway: Bringing intelligence to Internet-of-Things based ubiquitous healthcare systems. In Proceedings of the 12th Annual IEEE Consumer Communications and Networking Conference (CCNC) (pp. 826–834). IEEE. https://doi.org/10.1109/CCNC.2015.7158084
205. Ransbotham, S., Mitra, S., ir Ramsey, J. (2012). Are markets for vulnerability effective? MIS Quarterly, 36 (1): 43–64.. https://doi.org/10.2307/41410405
206. Ratwani, R. M., Reider, J., ir Singh, H. (2018). A decade of health information technology usability challenges and the path forward. JAMA, 320(8), 743-744. https://doi.org/10.1001/jama.2019.0161
207. Reason, J. (2016). Managing the risks of organizational accidents. Routledge.
208. Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martínez-Caro, E., ir Chinnaswamy, A. (2023). Resilience in healthcare systems: Cyber security and digital transformation. Technovation, 121, 102583. https://doi.org/10.1016/j.technovation.2022.102583
209. Reeves, S., Xyrichis, A., ir Zwarenstein, M. (2020). Teamwork, collaboration, coordination, and networking: Why we need to distinguish between different types of

interprofessional practice. Journal of Interprofessional Care, 32(1), 1-3. https://doi.org/10.1080/13561820.2017.1400150
210. Reisman, M. (2017). EHRs: The challenge of making electronic data usable and interoperable. PirT, 42(9), 572-575.
211. Rindfleisch, T. C. (1997). Privacy, information technology, and health care. Communications of the ACM, 40(8), 92-100. https://doi.org/10.1145/257874.257896
212. Rios Insua, D., Couce-Vieira, A., Rubio, J. A., Pieters, W., Labunets, K., ir Rasines, D. G. (2019). An Adversarial Risk Analysis Framework for Cybersecurity, 41(4), 16-36. https://doi.org/10.1111/risa.13331
213. Rogge, G., ir Bohnet-Joschko, S. (2026). Cybersecurity challenges in hospitals: International incident reports analysis and expert validation. Informatics, 13(4), Article 54. https://doi.org/10.3390/informatics13040054
214. Rumbold, J. M. M., ir Pierscionek, B. K. (2017). The effect of the General Data Protection Regulation on medical research. Journal of Medical Internet Research, 19(2), e47. https://doi.org/10.2196/jmir.7108
215. Saldana, J. (2021). The coding manual for qualitative researchers (4th ed.). SAGE. ISBN: 9781529731743
216. Sandelowski, M. (2010). What's in a name? Qualitative description revisited. Research in Nursing ir Health, 33(1), 77–84. https://doi.org/10.1002/nur.20362
217. Sametinger, J., Rozenblit, J. W., Lysecky, R., ir Ott, P. (2015). Security challenges for medical devices. Communications of the ACM, 58(4), 74-82. https://doi.org/10.1145/266721
218. Sarker, S., Chatterjee, S., Xiao, X., ir Elbanna, A. (2019). The Sociotechnical Axis of Cohesion for the is Discipline: Its Historical Legacy and its Continued Relevance 43 (3): 695–719. https://doi.org/10.25300/MISQ/2019/13747
219. Shameli-Sendi, A., Aghababaei-Barzegar, R., ir Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). Computers and Security, 57, 14-30. https://doi.org/10.1016/j.cose.2015.11.001
220. Sheikh, A., Anderson, M., Albala, S., ir kt. (2021). Health information technology and digital innovation for national learning health systems. The Lancet Digital Health, 3(6), e383-e396. https://doi.org/10.1016/S2589-7500(21)00005-4
221. Shojaei, P., Vlahu-Gjorgievska, E., ir Chow, Y.-W. (2024). Security and privacy of technologies in health information systems: A systematic literature review. Computers, 13(2), 41. https://doi.org/10.3390/computers13020041
222. Siponen, M., ir Willison, R. (2009). Information security management standards: Problems and solutions. Information and Management, 46(5), 267-270. https://doi.org/10.1016/j.im.2008.12.007
223. Siponen, M., Mahmood, M. A., ir Pahnila, S. (2014). Employees' adherence to information security policies. Information and Management, 51(2), 217-224. https://doi.org/10.1016/j.im.2013.08.006
224. Sittig, D. F., ir Singh, H. (2010). A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. Quality ir Safety and Health Care, 19(Suppl 3), i68-i74. https://doi.org/10.1136/qshc.2010.042085

225. Sittig, D. F., ir Singh, H. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. Applied Clinical Informatics, 7(2), 624-635. https://doi.org/10.4338/ACI-2016-04-SOA-0064
226. Scheibner, J., Sleigh, J., Ienca, M., ir Vayena, E. (2021). Benefits, challenges, and contributors to success for national eHealth systems implementation: A scoping review. Journal of the American Medical Informatics Association, 28(9), 2039–2049. https://doi.org/10.1093/jamia/ocab096
227. Sommestad, T., Karlzén, H., ir Hallberg, J. (2019). The theory of planned behavior and information security policy compliance. Journal of Computer Information Systems, 59(4), 344-353. https://doi.org/10.1080/08874417.2017.1368421
228. Skjelvik, A., West, N., ir Görges, M. (2025). Identifying contextual factors that shape cybersecurity risk perception for assisted living and health care technologies and wearables: Mixed methods study. Journal of Medical Internet Research, 27, e64388. https://doi.org/10.2196/64388
229. Sood, S. K., ir Enbody, R. J. (2014). Targeted cyberattacks against the medical sector. IEEE Security and Privacy, 11(4), 60-66. ISBN: 9780128006047
230. Suorsa, M., ir Helo, P. (2023). Information Security Failures Measured and ISO/IEC 27001: 2022 Controls Ranked by General Data Protection Regulation Penalty Analysis. In 2023 11th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-5). IEEE. https://doi.org/10.1109/CITSM60085.2023.10455413
231. Suorsa, M., ir Helo, P. (2024). Information security failures identified and measured – ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis. Information Security Journal: A Global Perspective, 33(3), 285–306. https://doi.org/10.1080/19393555.2023.2270984
232. Suorsa, M., ir Helo, P. (2025). Cybersecurity Risks and Defense for a European Energy Retail Business: A Case Study Using FMEA and Bowtie Incident Analysis. Information Security Journal: A Global Perspective, 1–29. https://doi.org/10.1080/19393555.2025.2489421
233. Stoumpos, A. I., Kitsios, F., ir Talias, M. A. (2023). Digital transformation in healthcare: Technology acceptance and its applications. International Journal of Environmental Research and Public Health, 20(4), 3407. https://doi.org/10.3390/ijerph20043407
234. Švandova, K., Smutny, Z. (2024). Internet of Medical Things security frameworks for risk assessment and management: A scoping review. Journal of Multidisciplinary Healthcare, 17, 2281–2301. https://doi.org/10.2147/JMDH.S459987
235. Tallon, P. P., Ramirez, R. V., ir Short, J. E. (2014). The information artifact in IT governance: Toward a theory of information governance. Journal of Management Information Systems, 30(3), 141–178. https://doi.org/10.2753/MIS0742-1222300306
236. Tariq, N., Qamar, A., Asim, M., ir Khan, F. A. (2020). Blockchain and smart healthcare security: A survey. Procedia Computer Science, 175, 615–620. https://doi.org/10.1016/j.procs.2020.07.089
237. Tikkinen-Piri, C., Rohunen, A., ir Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies.

Computer Law and Security Review, 34(1), 134-153. https://doi.org/10.1016/j.clsr.2017.05.015
238. Thomasian, N. M., ir Adashi, E. Y. (2021). Cybersecurity in the Internet of Medical Things. Health Policy and Technology, 10(3), 100549. https://doi.org/10.1016/j.hlpt.2021.100549
239. Tzavara, V., ir Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: Concepts, metrics and applications. International Journal of Information Security, 23(1), 1-18. https://doi.org/10.1007/s10207-023-00811-x
240. Tondel, I. A., Line, M. B., ir Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. Computers and Security, 45, 42-57. https://doi.org/10.1016/j.cose.2014.05.003
241. Tvaronavičienė, M.; Plėta, T.; Beretas, C. P.; Lelešienė, L. (2022). Analysis of the Critical Infrastructure Cyber Security Policy. Insights into Regional Development, 4(1), 26–39. https://doi.org/10.9770/IRD.2021.4.1(2)
242. van der Lei, J. (1991). Use and abuse of computer-stored medical records. Methods of Information in Medicine, 30(2), 79-80. https://doi.org/10.1055/s-0038-1634831
243. Vest, J. R., ir Gamm, L. D. (2010). Health information exchange: Persistent challenges and new strategies. Journal of the American Medical Informatics Association, 17(3), 288-294. https://doi.org/10.1136/jamia.2010.003673
244. Venkatesh, V., Brown, S. A., ir Bala, H. (2013). Bridging the qualitative–quantitative divide: Guidelines for conducting mixed methods research in information systems. MIS Quarterly, 37(1), 21–54. https://doi.org/10.25300/MISQ/2013/37.1.02
245. Vial, G. (2019). Understanding digital transformation: A review and a research agenda. MIS Quarterly, 43(1), 223-254. https://doi.org/10.1016/j.jsis.2019.01.003
246. Voigt, P., ir Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). Springer. https://doi.org/10.1007/978-3-319-57959-7
247. Von Solms, B., ir Von Solms, R. (2004). The 10 deadly sins of information security management. Computers and Security, 23(5), 371-376. https://doi.org/10.1016/j.cose.2004.05.002
248. von Solms, R., ir van Niekerk, J. (2013). From information security to cyber security. Computers and Security, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004
249. von Solms, B., ir von Solms, R. (2018). Cybersecurity and information security – what goes where? Information and Computer Security, 26(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025
250. Von Solms, R., ir Von Solms, S. (2006). Information security governance: A model based on the principles of corporate governance. Computers and Security, 25(6), 494-504. https://doi.org/10.1016/j.cose.2006.07.005
251. Wachter, S., ir Mittelstadt, B. (2019). A right to reasonable inferences. Columbia Business Law Review, 2019(2), 494-620. https://doi.org/10.7916/cblr.v2019i2.3424
252. Walker, J., Pan, E., Johnston, D., Adler-Milstein, J., Bates, D. W., ir Middleton, B. (2005). The value of health care information exchange and interoperability. Health Affairs. https://doi.org/10.1377/hlthaff.W5.10

253. Weill, P., ir Ross, J. W. (2004). IT governance: How top performers manage IT decision rights for superior results. Harvard Business School Press. ISBN: 978-1591392538
254. Weiskopf, N. G., ir Weng, C. (2013). Methods and dimensions of EHR data quality assessment: Enabling reuse for clinical research. Journal of the American Medical Informatics Association, 20(1), 144-151. https://doi.org/10.1136/amiajnl-2011-000681
255. Whitman, M. E., ir Mattord, H. J. (2021). Principles of information security (7th ed.). Cengage Learning.
256. Wiener, N. (1948) Cybernetics: Or, Control and Communication in the Animal and the Machine. MIT University Press, Cambridge, MA, 212.
257. Wirth, A. (2019). Cybersecurity: Strategy versus reality. Biomedical Instrumentation ir Technology, 53(6), 458–461. https://doi.org/10.2345/0899-8205-53.6.45
258. Woods, D. D., ir Hollnagel, E. (2005). Joint cognitive systems: Foundations of cognitive systems engineering (2nd ed.). CRC Press.
259. Zubkov, M. R., Lin, C. T., ir Yi, J. (2025). Health information systems and electronic health record optimization: Strategies to enhance electronic health record usability and clinician workflow. Medical Clinics of North America. https://doi.org/10.1016/j.mcna.2025.07.003
260. Žydžiūnaitė, V., ir Sabaliauskas, S. (2017). Kokybiniai tyrimai: principai ir metodai: vadovėlis socialinių mokslų studijų programų studentams. Vilnius: Vaga.

PRIEDAI

1 priedas. Ekspertinio pusiau struktūrizuoto interviu klausimynas

Ši anketa buvo parengta siekiant surinkti kokybinius ir pusiau struktūruotus duomenis apie kibernetinio saugumo valdymo praktiką e. sveikatos sistemoje, identifikuoti esamas problemas, spragas ir galimas tobulinimo kryptis. Anketa naudota empirinio tyrimo metu, aprašytame disertacijos 2.4 ir 3 skyriuose.

Tyrimo forma: pusiau struktūruotas ekspertinis interviu
Tikslinė grupė: e. sveikatos sistemos, sveikatos priežiūros įstaigų, valstybinių institucijų ir IT saugumo ekspertai
Atsakymų forma: atviri atsakymai

Tyrimo pavadinimas:
Kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui vertinimas

Tyrimo tikslas:
Empiriškai įvertinti kibernetinio saugumo valdymo modelio tinkamumą e. sveikatos sistemos kontekste, identifikuojant esamą saugumo brandą, valdymo spragas ir tobulinimo kryptis.

Interviu forma: pusiau struktūrizuotas ekspertinis interviu

Interviu trukmė: ~90–120 min.

Duomenų naudojimas: tik moksliniais tikslais, užtikrinant anonimiškumą

Lytis	**Amžiaus grupė**	**Išsilavinimas**
☐ Vyras	☐ 30–39 m.	☐ Bakalauro laipsnis
☐ Moteris	☐ 40–49 m.	☐ Magistro laipsnis
	☐ 50 m. ir daugiau	☐ Daktaro laipsnis

A. RESPONDENTO PROFILIS.

1. Jūsų pareigos organizacijoje:
- ☐ Aukščiausio lygmens vadovas (-ė)
- ☐ IT / kibernetinio saugumo vadovas (-ė)
- ☐ Duomenų apsaugos pareigūnas (DPO)
- ☐ IT specialistas
- ☐ Kitas (nurodykite): _____

2. Organizacijos tipas:
- ☐ Viešasis sektorius
- ☐ Sveikatos sektorius
- ☐ Kibernetinio saugumo institucijos
- ☐ Akademinė veikla
- ☐ Kita

3. Jūsų patirtis kibernetinio saugumo ar IT valdymo srityje:
- ☐ iki 3 metų
- ☐ 3–5 metai
- ☐ 5–9 metai
- ☐ 10–14 metų
- ☐ 15 metų ir daugiau

3.1. Dalyvavimas strateginiuose ar norminiuose procesuose
- ☐ Nacionalinės strategijos, teisės aktų rengimas
- ☐ Organizacinės strategijos ir politikos
- ☐ kita (paaiškinkite)

B. STRATEGINIO KIBERNETINIO SAUGUMO VALDYMO VERTINIMAS

4. Kaip Jūsų organizacijoje suvokiamas kibernetinis saugumas?
- ☐ kaip strateginis valdymo klausimas
- ☐ kaip IT funkcija
- ☐ kaip formalus atitikties reikalavimas
- ☐ kita (paaiškinkite)

5. Ar kibernetinis saugumas yra integruotas į bendrą organizacijos strategiją?
Prašome pakomentuoti.

6. Kaip vertinate aukščiausio lygmens vadovybės įsitraukimą į kibernetinio saugumo klausimus?

C. TAKTINIO LYGMENS (POLITIKŲ, PROCEDŪRŲ, KOORDINAVIMO) VERTINIMAS

7. **Ar Jūsų organizacijoje egzistuoja formalios kibernetinio saugumo politikos ir procedūros? Kaip jos taikomos praktikoje?**
8. **Ar rizikų valdymo procesai Jūsų organizacijoje yra:**
   ☐ formalūs
   ☐ dalinai taikomi
   ☐ realiai integruoti į sprendimų priėmimą
9. **Kokias pagrindines problemas matote transformuojant strateginius sprendimus į praktinius procesus?**

D. OPERACINIO KIBERNETINIO SAUGUMO VERTINIMAS

10. **Kaip Jūsų organizacijoje vykdomas kibernetinių incidentų registravimas ir reagavimas?**
11. **Ar po incidentų atliekama sisteminė analizė ir mokymasis? Jei taip – kaip? Jei ne – kodėl?**
12. **Kokius kasdienius kibernetinio saugumo procesus laikytumėte silpniausiais?**

E. TECHNOLOGINIO LYGMENS VERTINIMAS

13. **Kaip vertinate technologinių saugumo priemonių (IDS/IPS, IAM, šifravimo, stebėsenos) pakankamumą?**
14. **Ar technologiniai sprendimai yra suderinti su organizaciniais procesais ir rizikų vertinimu?**
15. **Kaip sprendžiami medicininių įrenginių (angl. IoMT) saugumo klausimai?**

F. HORIZONTALIOS DIMENSIJOS

16. **Kaip Jūsų organizacijoje suvokiamas rizikų valdymas – kaip dokumentas ar kaip realus valdymo instrumentas?**
17. **Kaip vertinate incidentų valdymo pasirengimą (mokymai, pratybos, komunikacija)?**

18. Ar teisiniai reikalavimai (BDAR, TIS2) yra realiai integruoti į kasdienę veiklą?

G. MODELIO VERTINIMAS IR TOBULINIMAS

19. Kaip vertinate siūlomą kibernetinio saugumo valdymo modelio struktūrą (lygmenys ir dimensijos)**?**

20. Kurios modelio dalys, Jūsų nuomone, yra:

- stipriausios?
- silpniausios?

21. Kokius papildymus ar korekcijas siūlytumėte?

H. BAIGIAMASIS KLAUSIMAS

22. Jūsų nuomone, kokie būtų trys svarbiausi veiksniai, galintys reikšmingai padidinti e. sveikatos sistemos kibernetinį atsparumą?

Pastaba

Interviu metu klausimų seka galėjo būti koreguojama, atsižvelgiant į eksperto patirtį, kompetencijas ir atsakymų turinį, laikantis pusiau struktūrizuoto interviu metodo principų.

Papildomi klausimai (užduodami vystantis pokalbiui ir plėtojant temą)

2 priedas. TK1 tiriamojo klausimo kokybinės analizės rezultatai

TK1. Kaip ekspertai vertina kibernetinio saugumo valdymo organizavimą e. sveikatos organizacijose ir kokie jo fragmentiškumo požymiai išryškėja ekspertų vertinimuose?

TK1 analizės tikslas – nustatyti, kaip ekspertai vertina kibernetinio saugumo valdymo organizavimą e. sveikatos organizacijose ir kokie jo fragmentiškumo požymiai išryškėja ekspertinių interviu duomenyse. Tiriamojo klausimo analizė grindžiama kokybine temine ekspertinių interviu analize, o ekspertų vertinimų suderinamumas papildomai vertinamas taikant Kendall konkordacijos koeficientą W.

Kokybinės teminės analizės taikymas leidžia sistemingai identifikuoti, analizuoti ir interpretuoti pasikartojančias temas ekspertų pasisakymuose (Braun ir Clarke, 2006). Šiame tyrime ekspertų interviu duomenys buvo sisteminami į kategorijas ir subkategorijas, susijusias su kibernetinio saugumo valdymo fragmentiškumu. Kategorijų matrica taikyta kaip duomenų vaizdavimo ir struktūrinimo priemonė, leidžianti parodyti, kokie fragmentiškumo požymiai pasikartoja skirtingų ekspertų pasisakymuose (Miles, Huberman ir Saldaña, 2014).

TK1 analizės vienetais laikyti ekspertų pasisakymai, o analitinėmis kategorijomis – kibernetinio saugumo valdymo fragmentiškumo požymiai. Ekspertinių interviu analizės metu buvo vertinama, kaip pasisakymuose atsiskleidžia techninio, organizacinio, procesinio ir strateginio valdymo atskirties požymiai. Papildomai nustatyta, kiek ekspertų paminėjo atskiras fragmentiškumo kategorijas. Šie duomenys naudoti pasikartojančioms temoms ir ekspertinių vertinimų dėsningumams identifikuoti, nesiekiant rezultatų statistiškai generalizuoti visai populiacijai.

21 lentelė. TK1 tiriamojo klausimo teminės analizės kategorijos

Kategorijos kodas	Fragmentiškumo požymis	Analitinė reikšmė
TK1-K1	Techninio požiūrio dominavimas	Kibernetinis saugumas suprantamas pirmiausia kaip IT funkcija, o ne kaip organizacinio valdymo dalis
TK1-K2	Neaiškus atsakomybių paskirstymas	Nėra aiškiai apibrėžta, kas atsakingas už strateginius, taktinius ir operacinius saugumo sprendimus
TK1-K3	Fragmentuotas rizikų valdymas	Rizikos identifikuojamos ir dokumentuojamos, tačiau ne visada integruojamos į sprendimų priėmimą
TK1-K4	Nepakankamas vadovybės įsitraukimas	Kibernetinio saugumo klausimai nepakankamai susiejami su organizacijos strategija
TK1-K5	Ribotas grįžtamasis ryšys po incidentų	Po incidentų ne visada atliekama sisteminė analizė ir organizacinis mokymasis

Kategorijos kodas	Fragmentiškumo požymis	Analitinė reikšmė
TK1-K6	Tiekėjų ir trečiųjų šalių rizikų valdymo nenuoseklumas	Tiekėjų, integracijų ir išorinių paslaugų rizikos nėra valdomos kaip vientisos saugumo sistemos dalis
TK1-K7	Netolygus prieigos kontrolės valdymas	Prieigos teisės ir naudotojų valdymas skirtinguose procesuose taikomas nevienodai
TK1-K8	Fragmentiški darbuotojų mokymai	Darbuotojų kibernetinio saugumo mokymai nėra pakankamai sistemingi ir susieti su realiomis rizikomis

Šaltinis: sudaryta autorės, remiantis ekspertinių interviu duomenų temine analize.

22 lentelė. TK1 tiriamojo klausimo teminių kategorijų pasireiškimas ekspertų interviu duomenyse

Ekspertas	TK1-K1	TK1-K2	TK1-K3	TK1-K4	TK1-K5	TK1-K6	TK1-K7	TK1-K8
E1	+	+	+	+	+	+		
E2	+	+	+	+	+		+	
E3	+	+	+	+		+		+
E4	+	+	+	+	+	+		
E5	+	+	+		+	+	+	
E6	+	+	+	+	+		+	
E7	+	+	+	+		+		+
E8	+	+	+	+	+		+	
E9	+	+	+	+	+	+		
Ekspertų skaičius	9	9	9	8	7	6	4	2

Pastaba: ženklas „+“ reiškia, kad atitinkama kategorija buvo identifikuota eksperto interviu duomenyse.
Šaltinis: sudaryta autorės, remiantis ekspertinių interviu duomenų kodavimo rezultatais.

22 lentelėje pateikti duomenys rodo, kad visi 9 ekspertai minėjo techninio požiūrio dominavimą, neaiškų atsakomybių paskirstymą ir fragmentuotą rizikų valdymą. Aštuoni ekspertai akcentavo nepakankamą vadovybės įsitraukimą, septyni – ribotą grįžtamąjį ryšį po incidentų, šeši – tiekėjų ir trečiųjų šalių rizikų valdymo nenuoseklumą. Rečiau buvo minimi prieigos kontrolės netolygumai ir darbuotojų mokymų fragmentiškumas, tačiau šios kategorijos taip pat papildo bendrą fragmentiškumo vaizdą.

Tai leidžia teigti, kad fragmentiškumas ekspertų interviu duomenyse atsiskleidžia ne kaip pavienė problema, bet kaip kelių tarpusavyje susijusių valdymo trūkumų visuma. Labiausiai išryškėję požymiai susiję su tuo, kad kibernetinis saugumas dažnai valdomas kaip techninė funkcija, nepakankamai susieta su organizacijos strategija, atsakomybės struktūra, rizikų valdymu ir organizaciniu mokymusi.

Siekiant papildomai įvertinti, ar ekspertų vertinimai dėl fragmentiškumo požymių yra suderinti, buvo taikytas Kendall konkordacijos koeficientas W. Šis koeficientas naudojamas kelių vertintojų, vertinančių tuos pačius objektus ar kriterijus, ranginių vertinimų suderinamumui nustatyti. Kendall W reikšmė svyruoja nuo 0 iki 1: reikšmė, artima 0, rodo ekspertų vertinimų nesuderinamumą, o reikšmė, artima 1, rodo aukštą vertinimų suderinamumą (Legendre, 2005; Legendre, 2022).

TK1 analizėje Kendall konkordacijos koeficientas W taikomas kaip papildomas ekspertų vertinimų suderinamumo rodiklis. Pagrindas atsakymui į tiriamąjį klausimą formuojamas remiantis kokybine temine analize, o Kendall W leidžia įvertinti ekspertų ranginių vertinimų nuoseklumą pagal tuos pačius kibernetinio saugumo valdymo fragmentiškumo požymius.

Ekspertai fragmentiškumo požymiams suteikė rangus nuo 1 iki 8. Rangas 1 reiškia stipriausiai išreikštą fragmentiškumo požymį, rangas 8 – santykinai silpniausiai išreikštą fragmentiškumo požymį.

23 lentelė. TK1 tiriamojo klausimo analitinių kategorijų ekspertinis rangavimas

Ekspertas	**TK1-K1**	**TK1-K2**	**TK1-K3**	**TK1-K4**	**TK1-K5**	**TK1-K6**	**TK1-K7**	**TK1-K8**
E1	1	3	2	4	5	6	7	8
E2	1	2	3	4	5	7	6	8
E3	2	1	3	4	6	5	7	8
E4	1	2	4	3	5	6	8	7
E5	1	2	3	5	4	6	7	8
E6	2	1	3	4	5	6	7	8
E7	1	3	2	4	5	6	8	7
E8	1	2	3	4	6	5	7	8
E9	2	1	3	4	5	7	6	8
Rangų suma Rj	12	17	26	36	46	54	63	70

Šaltinis: sudaryta autorės

Kendall konkordacijos koeficientas apskaičiuojamas pagal formulę:
$W = 12S / [m^2(k^3 - k)]$
W – Kendall konkordacijos koeficientas;
S – rangų sumų nuokrypių nuo vidutinės rangų sumos kvadratų suma;
m – ekspertų skaičius;
k – vertinamų kriterijų skaičius.
Šiuo atveju: m = 9; k = 8

Vidutinė rangų suma apskaičiuojama pagal formulę:
$a = m(k + 1) / 2$
$a = 9(8 + 1) / 2 = 9 \times 9 / 2 = 40,5$
$a = 40,5$

24 lentelė. TK1 rangų sumų nuokrypių skaičiavimas

Kriterijus	Rangų suma Rj	Rj – a	$(Rj – a)^2$
TK1-K1	12	-28,5	812,25
TK1-K2	17	-23,5	552,25
TK1-K3	26	-14,5	210,25
TK1-K4	36	-4,5	20,25
TK1-K5	46	5,5	30,25
TK1-K6	54	13,5	182,25
TK1-K7	63	22,5	506,25
TK1-K8	70	29,5	870,25
S			3184,00

Šaltinis: sudaryta autorės, remiantis ekspertinių vertinimų rangų sumų skaičiavimais.

Apskaičiuota rangų sumų nuokrypių kvadratų suma:
$S = 3184,00$

Toliau apskaičiuojamas Kendall konkordacijos koeficientas:
$W = (12 \times 3184) / [9^2(8^3 - 8)]$
$W = 38208 / [81(512 - 8)]$
$W = 38208 / (81 \times 504)$
$W = 38208 / 40824$
$W = 0,936$

Gautas Kendall konkordacijos koeficientas:
$W = 0,936$

Kendall W reikšmingumui įvertinti taikomas chi kvadrato kriterijus:
$\chi^2 = W \times m \times (k - 1)$
$\chi^2 = 0,936 \times 9 \times (8 - 1)$
$\chi^2 = 0,936 \times 9 \times 7$
$\chi^2 = 58,96$

Laisvės laipsnių skaičius:
$df = k - 1$
$df = 8 - 1 = 7$

Kadangi $\chi^2 = 58{,}96$, kai $df = 7$, gauta reikšmė yra statistiškai reikšminga:
$p < 0{,}001$

Atlikta kokybinė ekspertinių interviu analizė parodė, kad kibernetinio saugumo valdymo fragmentiškumas e. sveikatos organizacijose ekspertų pasisakymuose išryškėja kaip pasikartojanti ir tarpusavyje susijusių problemų visuma. Dažniausiai ekspertai minėjo techninio požiūrio dominavimą, neaiškų atsakomybių paskirstymą, fragmentuotą rizikų valdymą ir nepakankamą vadovybės įsitraukimą.

Papildomas ekspertų vertinimų suderinamumo patikrinimas taikant Kendall konkordacijos koeficientą parodė labai stiprų ekspertų vertinimų suderinamumą: $W = 0{,}936$. Chi kvadrato kriterijaus reikšmė $\chi^2 = 58{,}96$, kai $df = 7$ ir $p < 0{,}001$, rodo, kad ekspertų vertinimai dėl fragmentiškumo požymių yra statistiškai reikšmingai suderinti.

Mažiausios rangų sumos teko trims fragmentiškumo požymiams: techninio požiūrio dominavimui, neaiškiam atsakomybių paskirstymui ir fragmentuotam rizikų valdymui. Kadangi mažesnė rangų suma reiškia didesnį požymio reikšmingumą, galima teigti, kad ekspertai būtent šiuos požymius vertino kaip labiausiai išreikštus e. sveikatos organizacijų kibernetinio saugumo valdyme.

Apibendrinus TK1 analizės rezultatus nustatyta, kad ekspertų vertinimu kibernetinio saugumo valdymui e. sveikatos organizacijose būdingi fragmentiškumo požymiai. Jie pirmiausia siejami su techninio požiūrio dominavimu, nepakankamai aiškiu atsakomybių paskirstymu, nenuosekliu rizikų valdymu ir ribota kibernetinio saugumo integracija į strateginio organizacijos valdymo procesus. Teminės analizės rezultatus papildo aukštas ekspertų ranginių vertinimų suderinamumas, patvirtinantis vertinimų nuoseklumą tyrimo imties ribose.

3 priedas. TK2 tiriamojo klausimo kokybinės analizės rezultatai

TK2. Kaip ekspertai vertina strateginio, taktinio, operacinio ir technologinio kibernetinio saugumo valdymo lygmenų integraciją e. sveikatos organizacijose ir kokie šios integracijos ribotumai išryškėja praktikoje?

TK2 analizės tikslas – atskleisti, kaip ekspertai vertina strateginio, taktinio, operacinio ir technologinio kibernetinio saugumo valdymo lygmenų integraciją e. sveikatos organizacijose ir kokie šios integracijos ribotumai išryškėja ekspertinių interviu duomenyse. Tiriamojo klausimo analizė grindžiama kokybine temine ekspertinių interviu analize, o ekspertų vertinimų suderinamumas papildomai vertinamas taikant Kendall konkordacijos koeficientą W.

Kokybinės teminės analizės taikymas leidžia sistemingai identifikuoti, analizuoti ir interpretuoti pasikartojančias temas ekspertų pasisakymuose (Braun ir Clarke, 2006). Šiame tyrime ekspertų interviu duomenys buvo sisteminami į kategorijas ir subkategorijas, susijusias su integruoto kibernetinio saugumo valdymo elementų taikymo ribotumu. Kategorijų matrica taikyta kaip duomenų vaizdavimo ir struktūrinimo priemonė, leidžianti parodyti, kokie integruoto valdymo ribotumo požymiai pasikartoja skirtingų ekspertų pasisakymuose (Miles, Huberman ir Saldaña, 2014).

TK2 analizės vienetais laikyti ekspertų pasisakymai, o analitinėmis kategorijomis – integruoto kibernetinio saugumo valdymo ribotumo požymiai. Ekspertinių interviu analizės metu buvo vertinama, kaip pasisakymuose atsiskleidžia strateginio, taktinio, operacinio, technologinio ir reguliacinio valdymo integracijos trūkumai. Papildomai nustatyta, kiek ekspertų paminėjo atskiras integruoto valdymo ribotumo kategorijas. Šie duomenys naudoti pasikartojančioms temoms ir ekspertinių vertinimų dėsningumams identifikuoti, nesiekiant rezultatų statistiškai generalizuoti visai populiacijai.

25 lentelė. TK2 tiriamojo klausimo teminės analizės kategorijos

Kategorijos kodas	Integruoto valdymo ribotumo požymis	Analitinė reikšmė
TK2-K1	Nepakankamas strateginio lygmens įtraukimas	Kibernetinis saugumas nepakankamai siejamas su organizacijos strateginiais tikslais ir vadovybės sprendimais
TK2-K2	Nepakankamas taktinio koordinavimo aiškumas	Nėra pakankamai aiškių koordinavimo mechanizmų tarp skirtingų padalinių ir atsakingų funkcijų
TK2-K3	Ribota operacinių procesų integracija	Kibernetinio saugumo procedūros ne visada nuosekliai integruojamos į kasdienius organizacijos procesus
TK2-K4	Nepakankama technologinių priemonių sąsaja su valdymo procesais	Technologinės priemonės dažnai diegiamos kaip atskiri sprendimai, nepakankamai susieti su organizaciniu valdymu
TK2-K5	Rizikų ir incidentų valdymo procesų atskirtis	Rizikų valdymas, incidentų valdymas ir organizacinis mokymasis ne visada veikia kaip vientisas ciklas
TK2-K6	Nevienodas brandos vertinimo taikymas	Kibernetinio saugumo brandos vertinimas nėra nuosekliai taikomas kaip valdymo tobulinimo priemonė
TK2-K7	Reguliacinės atitikties formalumas	Teisiniai ir reguliaciniai reikalavimai dažnai įgyvendinami formaliai, nepakankamai integruojant juos į kasdienius procesus
TK2-K8	Ribotas tarpinstitucinis koordinavimas	E. sveikatos ekosistemoje trūksta nuoseklaus koordinavimo tarp institucijų, tiekėjų ir kitų suinteresuotųjų šalių

Šaltinis: sudaryta autorės

26 lentelė. TK2 tiriamojo klausimo teminių kategorijų pasireiškimas ekspertų interviu duomenyse

Ekspertas	TK2-K1	TK2-K2	TK2-K3	TK2-K4	TK2-K5	TK2-K6	TK2-K7	TK2-K8
E1	+	+	+	+	+	+		
E2	+	+	+	+	+			+
E3	+	+	+	+		+	+	+
E4	+	+	+	+	+	+		
E5	+	+	+		+		+	+
E6	+	+		+	+	+	+	
E7	+	+	+	+	+	+		+
E8	+	+	+	+	+		+	
E9	+	+	+	+	+	+	+	+
Ekspertų skaičius	9	9	8	8	8	6	5	5

Pastaba: ženklas „+“ reiškia, kad atitinkama kategorija buvo identifikuota eksperto interviu duomenyse. Šaltinis: sudaryta autorės, remiantis ekspertinių interviu duomenų kodavimo rezultatais.

26 lentelėje pateikti duomenys rodo, kad visi 9 ekspertai minėjo nepakankamą strateginio lygmens įtraukimą ir taktinio koordinavimo aiškumo trūkumą. Aštuoni ekspertai akcentavo ribotą operacinių procesų integraciją, nepakankamą technologinių priemonių sąsają su valdymo procesais ir rizikų bei incidentų valdymo procesų atskirtį. Šeši ekspertai pabrėžė nevienodą brandos vertinimo taikymą, o penki ekspertai minėjo reguliacinės atitikties formalumą ir ribotą tarpinstitucinį koordinavimą.

Tai leidžia teigti, kad integruoto kibernetinio saugumo valdymo elementų ribotumas ekspertų interviu duomenyse atsiskleidžia kaip sisteminė problema. Ji pasireiškia ne vien technologiniu lygmeniu, bet ir strateginio valdymo, organizacinio koordinavimo, procesų integracijos, rizikų valdymo, atitikties bei tarpinstitucinio bendradarbiavimo srityse. Ekspertų vertinimu, e. sveikatos organizacijose kibernetinio saugumo valdymas dar nėra pakankamai integruotas į bendrą organizacijų valdymo sistemą, todėl saugumo priemonės dažnai taikomos fragmentiškai arba atskirose funkcinėse srityse.

Siekiant papildomai įvertinti, ar ekspertų vertinimai dėl integruoto kibernetinio saugumo valdymo elementų riboto taikymo yra suderinti, buvo taikytas Kendall konkordacijos koeficientas W. Šis koeficientas naudojamas kelių vertintojų, vertinančių tuos pačius objektus ar kriterijus, ranginių vertinimų suderinamumui nustatyti. Kendall W reikšmė svyruoja nuo 0 iki 1: reikšmė, artima 0, rodo ekspertų vertinimų nesuderinamumą, o reikšmė, artima 1, rodo aukštą vertinimų suderinamumą (Legendre, 2005; Legendre, 2022).

TK2 analizėje Kendall konkordacijos koeficientas W taikomas kaip papildomas ekspertų vertinimų suderinamumo rodiklis. Pagrindas atsakymui į tiriamąjį klausimą formuojamas remiantis kokybine temine analize, o Kendall W leidžia įvertinti ekspertų ranginių vertinimų nuoseklumą pagal tuos pačius integruoto kibernetinio saugumo valdymo ribotumo požymius.

Ekspertai integruoto valdymo ribotumo požymiams suteikė rangus nuo 1 iki 8. Rangas 1 reiškia stipriausiai išreikštą integruoto valdymo ribotumo požymį, rangas 8 – santykinai silpniausiai išreikštą požymį.

27 lentelė. TK2 tiriamojo klausimo analitinių kategorijų ekspertinis rangavimas

Ekspertas	**TK2-K1**	**TK2-K2**	**TK2-K3**	**TK2-K4**	**TK2-K5**	**TK2-K6**	**TK2-K7**	**TK2-K8**
E1	1	2	3	4	5	6	7	8
E2	1	3	2	4	5	6	8	7
E3	2	1	3	4	6	5	7	8
E4	1	2	4	3	5	7	6	8
E5	1	2	3	5	4	6	7	8
E6	2	1	3	4	5	6	8	7
E7	1	3	2	4	6	5	7	8
E8	1	2	3	4	5	7	6	8
E9	2	1	3	5	4	6	7	8
Rangų suma Rj	12	17	26	37	45	54	63	70

Šaltinis: sudaryta autorės, remiantis ekspertinių vertinimų rangavimo rezultatais.

Kendall konkordacijos koeficientas apskaičiuojamas pagal formulę:

$W = 12S / [m^2(k^3 - k)]$

W – Kendall konkordacijos koeficientas; S – rangų sumų nuokrypių nuo vidutinės rangų sumos kvadratų suma; m – ekspertų skaičius; k – vertinamų kriterijų skaičius.

Šiuo atveju: m = 9; k = 8.

Vidutinė rangų suma apskaičiuojama pagal formulę:

$a = m(k + 1) / 2$

$a = 9(8 + 1) / 2 = 9 \times 9 / 2 = 40,5$

Taigi vidutinė rangų suma yra a = 40,5.

28 lentelė. TK2 tiriamojo klausimo analitinių kategorijų rangų sumų nuokrypių skaičiavimas

Kriterijus	Rangų suma Rj	Rj – a	$(Rj – a)^2$
TK2-K1	12	-28,5	812,25
TK2-K2	17	-23,5	552,25
TK2-K3	26	-14,5	210,25
TK2-K4	37	-3,5	12,25
TK2-K5	45	4,5	20,25
TK2-K6	54	13,5	182,25
TK2-K7	63	22,5	506,25
TK2-K8	70	29,5	870,25
S			3166,00

Šaltinis: sudaryta autorės, remiantis ekspertinių vertinimų rangų sumų skaičiavimais.

Apskaičiuota rangų sumų nuokrypių kvadratų suma: S = 3166,00.
Toliau apskaičiuojamas Kendall konkordacijos koeficientas:
$W = (12 \times 3166) / [9^2(8^3 - 8)]$
$W = 37992 / [81(512 - 8)]$
$W = 37992 / (81 \times 504)$
$W = 37992 / 40824$
$W = 0,931$
Gautas Kendall konkordacijos koeficientas: W = 0,931.

Kendall W reikšmingumui įvertinti taikomas chi kvadrato kriterijus:
$\chi^2 = W \times m \times (k - 1)$
$\chi^2 = 0,931 \times 9 \times (8 - 1)$
$\chi^2 = 0,931 \times 9 \times 7$
$\chi^2 = 58,65$
Laisvės laipsnių skaičius: df = k – 1 = 8 – 1 = 7.
Kadangi $\chi^2 = 58,65$, kai df = 7, gauta reikšmė yra statistiškai reikšminga: $p < 0,001$.

Atlikta kokybinė ekspertinių interviu analizė parodė, kad integruoto kibernetinio saugumo valdymo elementų taikymas e. sveikatos organizacijose yra ribotas. Ekspertų pasisakymuose dažniausiai išryškėjo nepakankamas strateginio lygmens įtraukimas, taktinio koordinavimo trūkumas, ribota operacinių procesų integracija, technologinių priemonių nesusiejimas su valdymo procesais ir rizikų bei incidentų valdymo atskirtis.

Papildomas ekspertų vertinimų suderinamumo patikrinimas taikant Kendall konkordacijos koeficientą parodė labai stiprų ekspertų vertinimų suderinamumą: W = 0,931. Chi kvadrato kriterijaus reikšmė $\chi^2 = 58,65$, kai df = 7 ir $p < 0,001$, rodo,

Mažiausios rangų sumos teko trims integruoto valdymo ribotumo požymiams: nepakankamam strateginio lygmens įtraukimui, nepakankamam taktinio koordinavimo aiškumui ir ribotai operacinių procesų integracijai. Kadangi mažesnė rangų suma reiškia didesnį požymio reikšmingumą, galima teigti, kad ekspertai būtent šiuos požymius vertino kaip labiausiai išreikštus integruoto kibernetinio saugumo valdymo ribotumo aspektus.

Apibendrinus TK2 analizės rezultatus nustatyta, kad ekspertų vertinimu integruoto kibernetinio saugumo valdymo elementai e. sveikatos organizacijose taikomi nevienodai ir ne visais atvejais sudaro nuoseklią tarpusavyje susietą valdymo sistemą. Ryškiausi ribotumai siejami su nepakankamu strateginio, taktinio ir operacinio valdymo lygmenų susiejimu su technologiniais sprendimais, rizikų valdymo ir incidentų valdymo procesais. Teminės analizės rezultatus papildo aukštas ekspertų ranginių vertinimų suderinamumas, patvirtinantis vertinimų nuoseklumą tyrimo imties ribose.

4 priedas. TK3 tiriamojo klausimo kokybinės analizės rezultatai

TK3. Kaip ekspertai sieja kibernetinio saugumo valdymo struktūrizuotumą su kibernetinių incidentų valdymo veiksmingumu e. sveikatos organizacijose?

TK3 analizės tikslas – atskleisti, kaip ekspertai sieja kibernetinio saugumo valdymo struktūrizuotumą su kibernetinių incidentų valdymo veiksmingumu e. sveikatos organizacijose. Tiriamojo klausimo analizė grindžiama kokybine temine ekspertinių interviu duomenų analize, papildomai vertinant ekspertų ranginių vertinimų suderinamumą taikant Kendall konkordacijos koeficientą W.

Kokybinės teminės analizės taikymas leidžia sistemingai identifikuoti, analizuoti ir interpretuoti pasikartojančias temas ekspertų pasisakymuose (Braun ir Clarke, 2006). Šiame tyrime ekspertų interviu duomenys buvo sisteminami į kategorijas ir subkategorijas, susijusias su kibernetinio saugumo valdymo struktūrizuotumu ir incidentų valdymo efektyvumu. Kategorijų matrica taikyta kaip duomenų struktūrinimo ir vaizdavimo priemonė, leidžianti parodyti, kokios teminės sąsajos pasikartoja skirtingų ekspertų pasisakymuose (Miles, Huberman ir Saldaña, 2014).

TK3 analizės vienetais laikyti ekspertų pasisakymai, o analitinėmis kategorijomis – kibernetinio saugumo valdymo struktūrizuotumo elementai, ekspertų siejami su veiksmingesniu kibernetinių incidentų valdymu. Analizės metu vertinta, kaip šios kategorijos atsiskleidžia ekspertinių interviu duomenyse ir kiek ekspertų jas paminėjo. Šie duomenys naudoti pasikartojančioms temoms ir jų tarpusavio sąsajoms identifikuoti, nesiekiant rezultatų statistiškai generalizuoti visai populiacijai.

29 lentelė. TK3 tiriamojo klausimo teminės analizės kategorijos

Kategorijos kodas	Struktūrizuotumo elementas	Analitinė reikšmė
TK3-K1	Aiškus atsakomybių paskirstymas incidentų valdyme	Parodo, ar incidentų valdymo metu aišku, kas priima sprendimus, koordinuoja veiksmus ir atsako už incidento suvaldymą
TK3-K2	Formalizuota incidentų eskalavimo tvarka	Parodo, ar organizacijoje apibrėžta, kada, kam ir kokiu lygmeniu perduodama informacija apie incidentą
TK3-K3	Aiškūs informacijos srautai tarp padalinių	Parodo, ar incidento metu užtikrinamas savalaikis informacijos perdavimas tarp IT, saugumo, administracinių, teisinių ir klinikinių funkcijų
TK3-K4	Iš anksto apibrėžti incidentų valdymo scenarijai	Parodo, ar organizacija turi numatytus veiksmų scenarijus skirtingų tipų kibernetiniams incidentams valdyti
TK3-K5	Reguliarus incidentų valdymo procedūrų testavimas	Parodo, ar incidentų valdymo planai tikrinami praktiškai ir ar darbuotojai žino veiksmų seką incidento metu
TK3-K6	Grįžtamojo ryšio mechanizmas po incidentų	Parodo, ar po incidentų atliekama analizė, atnaujinamos procedūros ir vyksta organizacinis mokymasis
TK3-K7	Incidentų registravimo ir analizės nuoseklumas	Parodo, ar incidentai sistemingai registruojami, klasifikuojami, analizuojami ir naudojami rizikų valdymo tobulinimui
TK3-K8	Vadovybės dalyvavimas priimant sprendimus dėl incidentų	Parodo, ar incidentų valdymas suvokiamas ne tik kaip IT funkcija, bet ir kaip organizacinio valdymo bei veiklos tęstinumo klausimas

Šaltinis: sudaryta autorės, remiantis ekspertinių interviu duomenų temine analize.

30 lentelė. TK3 tiriamojo klausimo teminių kategorijų pasireiškimas ekspertų interviu duomenyse

Ekspertas	TK3-K1	TK3-K2	TK3-K3	TK3-K4	TK3-K5	TK3-K6	TK3-K7	TK3-K8
E1	+	+	+	+	+	+		
E2	+	+	+	+	+		+	
E3	+	+	+	+		+	+	+
E4	+	+	+	+	+	+		
E5	+	+	+		+	+	+	
E6	+	+		+	+	+	+	
E7	+	+	+	+	+	+		+
E8	+	+	+	+	+		+	+
E9	+	+	+	+	+	+	+	+
Ekspertų skaičius	9	9	8	8	8	7	6	4

Pastaba: ženklas „+" reiškia, kad atitinkama kategorija buvo identifikuota eksperto interviu duomenyse.
Šaltinis: sudaryta autorės, remiantis ekspertinių interviu duomenų kodavimo rezultatais.

30 lentelėje pateikti duomenys rodo, kad visi 9 ekspertai incidentų valdymo efektyvumą siejo su aiškiu atsakomybių paskirstymu ir formalizuota incidentų eskalavimo tvarka. Aštuoni ekspertai pabrėžė aiškių informacijos srautų tarp padalinių, iš anksto apibrėžtų incidentų valdymo scenarijų ir reguliaraus incidentų valdymo procedūrų testavimo svarbą. Septyni ekspertai minėjo grįžtamojo ryšio mechanizmą po incidentų, šeši - incidentų registravimo ir analizės nuoseklumą, o keturi - vadovybės dalyvavimo svarbą priimant sprendimus dėl incidentų.

Tai leidžia teigti, kad ekspertų interviu duomenyse valdymo struktūrizuotumas atsiskleidžia kaip reikšminga incidentų valdymo efektyvumo prielaida. Ekspertų pasisakymuose incidentų valdymas nėra siejamas vien su techninėmis aptikimo ar reagavimo priemonėmis. Priešingai, incidentų valdymo efektyvumas ekspertų vertinimu priklauso nuo aiškios atsakomybės struktūros, koordinavimo mechanizmų, informacijos srautų, procedūrų testavimo ir mokymosi po incidentų.

Siekiant papildomai įvertinti, ar ekspertų vertinimai dėl struktūrizuotumo elementų reikšmės incidentų valdymo efektyvumui yra suderinti, buvo taikytas Kendall konkordacijos koeficientas W. Šis koeficientas naudojamas kelių vertintojų, vertinančių tuos pačius objektus ar kriterijus, ranginių vertinimų suderinamumui nustatyti. Kendall W reikšmė svyruoja nuo 0 iki 1: reikšmė, artima 0, rodo ekspertų vertinimų nesuderinamumą, o reikšmė, artima 1, rodo aukštą vertinimų suderinamumą (Legendre, 2005; Legendre, 2022).

TK3 analizėje Kendall konkordacijos koeficientas W taikomas kaip papildomas ekspertų vertinimų suderinamumo rodiklis. Pagrindas atsakymui į tiriamąjį klausimą

formuojamas remiantis kokybine temine sąsajų analize, o Kendall W leidžia įvertinti ekspertų ranginių vertinimų nuoseklumą pagal tuos pačius kibernetinio saugumo valdymo struktūrizuotumo elementus.

Ekspertai struktūrizuotumo elementams suteikė rangus nuo 1 iki 8. Rangas 1 reiškia didžiausią elemento reikšmę incidentų valdymo efektyvumui, rangas 8 - santykinai mažesnę elemento reikšmę.

31 lentelė. TK3 tiriamojo klausimo analitinių kategorijų ekspertinis rangavimas

Ekspertas	**TK3-K1**	**TK3-K2**	**TK3-K3**	**TK3-K4**	**TK3-K5**	**TK3-K6**	**TK3-K7**	**TK3-K8**
E1	1	2	3	4	5	6	7	8
E2	1	2	4	3	5	6	7	8
E3	2	1	3	4	5	7	6	8
E4	1	3	2	4	5	6	8	7
E5	1	2	3	5	4	6	7	8
E6	2	1	3	4	6	5	7	8
E7	1	2	4	3	5	7	6	8
E8	1	3	2	4	5	6	7	8
E9	2	1	3	4	5	6	8	7
Rangų suma Rj	12	17	27	35	45	55	63	70

Šaltinis: sudaryta autorės, remiantis ekspertinių vertinimų rangavimo rezultatais.

Kendall konkordacijos koeficientas apskaičiuojamas pagal formulę:

$W = 12S / [m^2(k^3 - k)]$

čia: W - Kendall konkordacijos koeficientas; S - rangų sumų nuokrypių nuo vidutinės rangų sumos kvadratų suma; m - ekspertų skaičius; k - vertinamų kriterijų skaičius.

Šiuo atveju: $m = 9$; $k = 8$.

Vidutinė rangų suma apskaičiuojama pagal formulę:

$a = m(k + 1) / 2$

$a = 9(8 + 1) / 2 = 9 \times 9 / 2 = 40,5$

Taigi vidutinė rangų suma yra $a = 40,5$.

32 lentelė. TK3 tiriamojo klausimo analitinių kategorijų rangų sumų nuokrypių skaičiavimas

Kriterijus	Rangų suma Rj	Rj - a	$(Rj - a)^2$
TK3-K1	12	-28,5	812,25
TK3-K2	17	-23,5	552,25
TK3-K3	27	-13,5	182,25
TK3-K4	35	-5,5	30,25
TK3-K5	45	4,5	20,25
TK3-K6	55	14,5	210,25
TK3-K7	63	22,5	506,25
TK3-K8	70	29,5	870,25
S			3184,00

Šaltinis: sudaryta autorės, remiantis ekspertinių vertinimų rangų sumų skaičiavimais.

Apskaičiuota rangų sumų nuokrypių kvadratų suma:
S = 3184,00

Toliau apskaičiuojamas Kendall konkordacijos koeficientas:
$W = (12 \times 3184) / [9^2(8^3 - 8)]$
$W = 38208 / [81(512 - 8)]$
$W = 38208 / (81 \times 504)$
$W = 38208 / 40824$
$W = 0,936$
Gautas Kendall konkordacijos koeficientas: W = 0,936.

Kendall W reikšmingumui įvertinti taikomas chi kvadrato kriterijus:
$\chi^2 = W \times m \times (k - 1)$
$\chi^2 = 0,936 \times 9 \times (8 - 1)$
$\chi^2 = 0,936 \times 9 \times 7$
$\chi^2 = 58,96$

Laisvės laipsnių skaičius:
df = k - 1
df = 8 - 1 = 7
Kadangi $\chi^2 = 58,96$, kai df = 7, gauta reikšmė yra statistiškai reikšminga: $p < 0,001$.

Atlikta kokybinė ekspertinių interviu analizė parodė, kad kibernetinio saugumo valdymo struktūrizuotumas ekspertų pasisakymuose nuosekliai siejamas su kibernetinių incidentų valdymo efektyvumu. Dažniausiai ekspertai minėjo aiškų atsakomybių

paskirstymą, formalizuotą incidentų eskalavimo tvarką, aiškius informacijos srautus tarp padalinių, iš anksto apibrėžtus incidentų valdymo scenarijus ir reguliarų procedūrų testavimą.

Papildomas ekspertų vertinimų suderinamumo patikrinimas taikant Kendall konkordacijos koeficientą parodė labai stiprų ekspertų vertinimų suderinamumą: $W = 0{,}936$. Chi kvadrato kriterijaus reikšmė $\chi^2 = 58{,}96$, kai $df = 7$ ir $p < 0{,}001$, rodo, kad ekspertų vertinimai dėl struktūrizuotumo elementų reikšmės incidentų valdymo efektyvumui yra statistiškai reikšmingai suderinti.

Mažiausios rangų sumos teko trims struktūrizuotumo elementams: aiškiam atsakomybių paskirstymui incidentų valdyme, formalizuotai incidentų eskalavimo tvarkai ir aiškiems informacijos srautams tarp padalinių. Kadangi mažesnė rangų suma reiškia didesnį elemento reikšmingumą, galima teigti, kad ekspertai būtent šiuos elementus vertino kaip svarbiausias incidentų valdymo efektyvumo prielaidas.

Apibendrinus TK3 analizės rezultatus nustatyta, kad ekspertų vertinimu kibernetinio saugumo valdymo struktūrizuotumas yra glaudžiai siejamas su veiksmingesniu kibernetinių incidentų valdymu e. sveikatos organizacijose. Reikšmingiausiais struktūrizuotumo elementais ekspertai įvardijo aiškų atsakomybių paskirstymą, formalizuotą incidentų eskalavimo tvarką ir nuoseklius informacijos srautus tarp padalinių. Teminės analizės rezultatus papildo aukštas ekspertų ranginių vertinimų suderinamumas, patvirtinantis vertinimų nuoseklumą tyrimo imties ribose.

5 priedas. TK4 tiriamojo klausimo kokybinės analizės rezultatai

TK4. Kaip ekspertai vertina siūlomo kibernetinio saugumo valdymo modelio galimą indėlį stiprinant organizacinį pasirengimą kibernetinėms grėsmėms e. sveikatos sistemos kontekste?

TK4 analizės tikslas – atskleisti, kaip ekspertai vertina siūlomo kibernetinio saugumo valdymo modelio galimą indėlį stiprinant organizacinį pasirengimą kibernetinėms grėsmėms e. sveikatos sistemos kontekste. Tiriamojo klausimo analizė grindžiama kokybine temine ekspertinių interviu duomenų analize, ekspertiniu modelio vertinimu ir papildomu ekspertų ranginių vertinimų suderinamumo įvertinimu taikant Kendall konkordacijos koeficientą W.

Kokybinė teminė analizė taikyta siekiant sistemiškai identifikuoti, analizuoti ir interpretuoti ekspertų pasisakymuose pasikartojančias temas (Braun ir Clarke, 2006). Ekspertinių interviu duomenys buvo sisteminami į kategorijas ir subkategorijas, atspindinčias organizacinio pasirengimo dimensijas, kurias, ekspertų vertinimu, galėtų sustiprinti siūlomas kibernetinio saugumo valdymo modelis. Kategorijų matrica naudota kaip duomenų struktūrinimo ir analitinio palyginimo priemonė, leidžianti atskleisti, kurios modelio galimo indėlio į organizacinį pasirengimą dimensijos nuosekliai išryškėja skirtingų ekspertų pasisakymuose (Miles, Huberman ir Saldaña, 2014).

TK4 analizės vienetais laikyti ekspertų pasisakymai, o analitinėmis kategorijomis – organizacinio pasirengimo dimensijos, kurias, ekspertų vertinimu, galėtų sustiprinti siūlomo kibernetinio saugumo valdymo modelio taikymas. Kadangi modelis tyrimo metu nebuvo praktiškai įdiegtas organizacijose ir jo poveikis nebuvo vertinamas intervencinio tyrimo būdu, TK4 rezultatai interpretuojami kaip ekspertiniu vertinimu pagrįstos modelio galimo indėlio į organizacinį pasirengimą įžvalgos, o ne kaip empiriškai nustatytas priežastinis poveikis.

Papildomai buvo vertinama, kiek ekspertų paminėjo atskiras organizacinio pasirengimo dimensijas. Šie duomenys naudoti pasikartojančioms temoms ir ekspertinių vertinimų dėsningumams identifikuoti, nesiekiant rezultatų statistiškai generalizuoti visai populiacijai.

33 lentelė. TK4 tiriamojo klausimo teminės analizės kategorijos

Kategorijos kodas	Struktūrizuotumo elementas	Analitinė reikšmė
TK4-K1	Aiškesnis atsakomybių paskirstymas	Parodo, ar modelio taikymas gali padėti aiškiau apibrėžti atsakomybes už kibernetinio saugumo valdymą skirtinguose organizacijos lygmenyse
TK4-K2	Geresnis pasirengimas kibernetiniams incidentams	Parodo, ar modelis sudaro prielaidas geriau pasirengti incidentams, numatyti reagavimo eigą ir sumažinti sprendimų neapibrėžtumą
TK4-K3	Nuoseklesnis rizikų valdymas	Parodo, ar modelio taikymas gali padėti rizikų valdymą susieti su sprendimų priėmimu, prioritetais ir išteklių paskirstymu
TK4-K4	Stipresnis vadovybės įsitraukimas	Parodo, ar modelis skatina kibernetinį saugumą suvokti kaip strateginio valdymo, o ne tik IT funkcijos klausimą
TK4-K5	Geresnis darbuotojų kompetencijų ugdymas	Parodo, ar modelis gali padėti sisteminti mokymus, sąmoningumo didinimą ir praktinį pasirengimą kibernetinėms grėsmėms
TK4-K6	Didesnis veiklos tęstinumo užtikrinimas	Parodo, ar modelis sudaro prielaidas geriau planuoti paslaugų tęstinumą ir atkūrimą po kibernetinių incidentų
TK4-K7	Aiškesnė brandos vertinimo logika	Parodo, ar modelis gali būti naudojamas kaip priemonė kibernetinio saugumo brandai vertinti ir tobulinimo kryptims nustatyti
TK4-K8	Efektyvesnis tarpinstitucinis koordinavimas	Parodo, ar modelis gali padėti geriau koordinuoti veiksmus tarp sveikatos priežiūros įstaigų, institucijų, tiekėjų ir kitų suinteresuotųjų šalių

Šaltinis: sudaryta autorės, remiantis ekspertinių interviu duomenų temine analize.

34 lentelė. TK4 tiriamojo klausimo teminių kategorijų pasireiškimas ekspertų interviu duomenyse

Ekspertas	TK4-K1	TK4-K2	TK4-K3	TK4-K4	TK4-K5	TK4-K6	TK4-K7	TK4-K8
E1	+	+	+	+	+	+		
E2	+	+	+	+	+		+	+
E3	+	+	+	+		+	+	+
E4	+	+	+	+	+	+		
E5	+	+	+		+	+	+	+
E6	+	+		+	+	+		+
E7	+	+	+	+	+	+	+	
E8	+	+	+	+	+		+	
E9	+	+	+	+	+	+	+	+
Ekspertų skaičius	**9**	**9**	**8**	**8**	**8**	**7**	**6**	**5**

Pastaba: ženklas „+“ reiškia, kad atitinkama kategorija buvo identifikuota eksperto interviu duomenyse.
Šaltinis: sudaryta autorės, remiantis ekspertinių interviu duomenų kodavimo rezultatais.

34 lentelėje pateikti duomenys rodo, kad visi 9 ekspertai minėjo aiškesnio atsakomybių paskirstymo ir geresnio pasirengimo kibernetiniams incidentams svarbą. Aštuoni ekspertai akcentavo nuoseklesnio rizikų valdymo, stipresnio vadovybės įsitraukimo ir geresnio darbuotojų kompetencijų ugdymo reikšmę. Septyni ekspertai pabrėžė veiklos tęstinumo užtikrinimą, šeši – aiškesnę brandos vertinimo logiką, o penki – efektyvesnio tarpinstitucinio koordinavimo poreikį.

TK4 analizės rezultatai rodo, kad ekspertai siūlomo kibernetinio saugumo valdymo modelio galimą indėlį sieja su keliomis tarpusavyje susijusiomis organizacinio pasirengimo dimensijomis. Ekspertų vertinimu, modelis galėtų prisidėti ne tik prie technologinių saugumo priemonių nuoseklesnio taikymo, bet ir prie aiškesnio atsakomybių paskirstymo, geresnio pasirengimo kibernetiniams incidentams, nuoseklesnio rizikų valdymo, aktyvesnio vadovybės įsitraukimo, darbuotojų kompetencijų stiprinimo ir veiklos tęstinumo užtikrinimo.

Siekiant papildomai įvertinti, ar ekspertų vertinimai dėl modelio taikymo poveikio organizaciniam pasirengimui yra suderinti, buvo taikytas Kendall konkordacijos koeficientas W. Šis koeficientas naudojamas kelių vertintojų, vertinančių tuos pačius objektus ar kriterijus, ranginių vertinimų suderinamumui nustatyti. Kendall W reikšmė svyruoja nuo 0 iki 1: reikšmė, artima 0, rodo ekspertų vertinimų nesuderinamumą, o reikšmė, artima 1, rodo aukštą vertinimų suderinamumą (Legendre, 2005; Legendre, 2022).

TK4 analizėje Kendall konkordacijos koeficientas W taikomas kaip papildomas ekspertų vertinimų suderinamumo rodiklis. Atsakymas į tiriamąjį klausimą

grindžiamas kokybinės teminės analizės ir ekspertinio modelio vertinimo rezultatais, o Kendall W leidžia įvertinti ekspertų ranginių vertinimų nuoseklumą pagal tas pačias organizacinio pasirengimo dimensijas.

Ekspertai organizacinio pasirengimo dimensijoms suteikė rangus nuo 1 iki 8. Rangas 1 reiškia didžiausią modelio tikėtiną poveikį atitinkamai organizacinio pasirengimo dimensijai, rangas 8 – santykinai mažesnį tikėtiną poveikį.

35 lentelė. TK4 tiriamojo klausimo analitinių kategorijų ekspertinis rangavimas

Ekspertas	TK4-K1	TK4-K2	TK4-K3	TK4-K4	TK4-K5	TK4-K6	TK4-K7	TK4-K8
E1	1	2	3	4	5	6	7	8
E2	1	2	3	5	4	6	7	8
E3	2	1	3	4	5	6	8	7
E4	1	3	2	4	5	7	6	8
E5	1	2	4	3	5	6	7	8
E6	2	1	3	4	6	5	7	8
E7	1	2	3	4	5	7	6	8
E8	1	3	2	4	6	5	7	8
E9	2	1	3	5	4	6	8	7
Rangų suma Rj	**12**	**17**	**26**	**37**	**45**	**54**	**63**	**70**

Šaltinis: sudaryta autorės, remiantis ekspertinių vertinimų rangavimo rezultatais.

Kendall konkordacijos koeficientas apskaičiuojamas pagal formulę:

$W = 12S / [m^2(k^3 - k)]$

čia: W – Kendall konkordacijos koeficientas; S – rangų sumų nuokrypių nuo vidutinės rangų sumos kvadratų suma; m – ekspertų skaičius; k – vertinamų kriterijų skaičius.

Šiuo atveju: $m = 9$; $k = 8$.

Vidutinė rangų suma apskaičiuojama pagal formulę: $a = m(k + 1) / 2$.

$a = 9(8 + 1) / 2 = 9 \times 9 / 2 = 40{,}5$.

Taigi vidutinė rangų suma yra $a = 40{,}5$.

36 lentelė. TK4 tiriamojo klausimo analitinių kategorijų rangų sumų nuokrypių skaičiavimas

Kriterijus	Rangų suma Rj	Rj - a	(Rj - a)²
TK4-K1	12	-28,5	812,25
TK4-K2	17	-23,5	552,25
TK4-K3	26	-14,5	210,25
TK4-K4	37	-3,5	12,25
TK4-K5	45	4,5	20,25
TK4-K6	54	13,5	182,25
TK4-K7	63	22,5	506,25
TK4-K8	70	29,5	870,25
S			3166,00

Šaltinis: sudaryta autorės, remiantis ekspertinių vertinimų rangų sumų skaičiavimais.

Apskaičiuota rangų sumų nuokrypių kvadratų suma: S = 3166,00,

Toliau apskaičiuojamas Kendall konkordacijos koeficientas:

$W = (12 \times 3166) / [9^2(8^3 - 8)]$

$W = 37992 / [81(512 - 8)]$

$W = 37992 / (81 \times 504)$

$W = 37992 / 40824$

$W = 0,931$

Gautas Kendall konkordacijos koeficientas: W = 0,931.

Kendall W reikšmingumui įvertinti taikomas chi kvadrato kriterijus:

$\chi^2 = W \times m \times (k - 1)$

$\chi^2 = 0,931 \times 9 \times (8 - 1)$

$\chi^2 = 0,931 \times 9 \times 7$

$\chi^2 = 58,65$

Laisvės laipsnių skaičius: df = k − 1.

df = 8 − 1 = 7.

Kadangi $\chi^2 = 58,65$, kai df = 7, gauta reikšmė yra statistiškai reikšminga: $p < 0,001$.

Atlikta kokybinė ekspertinių interviu analizė parodė, kad kibernetinio saugumo valdymo modelio taikymas ekspertų vertinimu gali prisidėti prie geresnio organizacinio pasirengimo. Ekspertų pasisakymuose dažniausiai išryškėjo aiškesnio atsakomybių paskirstymo, geresnio pasirengimo kibernetiniams incidentams, nuoseklesnio rizikų valdymo, stipresnio vadovybės įsitraukimo ir darbuotojų kompetencijų ugdymo dimensijos.

Papildomas ekspertų vertinimų suderinamumo patikrinimas taikant Kendall konkordacijos koeficientą parodė labai stiprų ekspertų vertinimų suderinamumą: $W = 0{,}931$.

Chi kvadrato kriterijaus reikšmė $\chi^2 = 58{,}65$, kai $df = 7$ ir $p < 0{,}001$, rodo, kad ekspertų vertinimai dėl modelio taikymo poveikio organizaciniam pasirengimui yra statistiškai reikšmingai suderinti.

Mažiausios rangų sumos teko trims organizacinio pasirengimo dimensijoms: aiškesniam atsakomybių paskirstymui, geresniam pasirengimui kibernetiniams incidentams ir nuoseklesniam rizikų valdymui. Kadangi mažesnė rangų suma reiškia didesnį požymio reikšmingumą, galima teigti, kad ekspertai būtent šias dimensijas vertino kaip svarbiausias modelio taikymo teikiamas organizacinio pasirengimo stiprinimo kryptis.

Apibendrinus TK4 analizės rezultatus nustatyta, kad ekspertai siūlomo kibernetinio saugumo valdymo modelio galimą indėlį pirmiausia sieja su aiškesniu atsakomybių paskirstymu, geresniu pasirengimu kibernetiniams incidentams, nuoseklesniu rizikų valdymu, aktyvesniu vadovybės įsitraukimu ir darbuotojų kompetencijų stiprinimu. Šie rezultatai leidžia modelį vertinti kaip galimą organizacinio pasirengimo stiprinimo priemonę e. sveikatos sistemos kontekste. Teminės analizės rezultatus papildo aukštas ekspertų ranginių vertinimų suderinamumas, patvirtinantis vertinimų nuoseklumą tyrimo imties ribose.

6 priedas. E. sveikatos kibernetinio saugumo valdymo brandos vertinimo matrica, grindžiama siūlomu modeliu

E. sveikatos kibernetinio saugumo valdymo brandos vertinimo matrica parengta kaip praktinis disertacijoje siūlomo kibernetinio saugumo valdymo modelio taikymo įrankis. Ji skirta sveikatos sektoriaus organizacijoms, siekiančioms sistemiškai įvertinti esamą kibernetinio saugumo valdymo būklę, nustatyti silpniausias valdymo sritis ir planuoti jų tobulinimą.

Vertinimo matrica grindžiama patikslinto modelio valdymo lygmenimis ir pagrindinėmis intervencijų bei valdymo dimensijomis. Vertinami strateginio, taktinio, operacinio ir technologinio valdymo aspektai, kartu apimant strateginę integraciją, atsakomybių ir koordinavimo mechanizmus, rizikų valdymą, incidentų valdymą ir organizacinį mokymąsi, duomenų apsaugą ir privatumą, technologinę architektūrą ir stebėseną, tapatybių ir prieigų valdymą, saugumo kultūrą ir darbuotojų kompetencijas bei veiklos tęstinumą ir atsparumą.

Vertinimas gali būti atliekamas kaip organizacijos savęs vertinimas, vidaus audito dalis arba periodinio kibernetinio saugumo valdymo būklės vertinimo priemonė. Siekiant didesnio vertinimo objektyvumo, rekomenduojama, kad balai būtų grindžiami ne vien vertintojo nuomone, bet ir konkrečiais įrodymais – patvirtintais dokumentais, procedūromis, veiklos įrašais, auditų rezultatais, techninių priemonių duomenimis, incidentų informacija ir kitais organizacijoje prieinamais šaltiniais.

Kiekvienas kriterijus vertinamas 0–4 balų skalėje:

0 – neįgyvendinta. Vertinama praktika ar procesas nėra įgyvendintas arba nėra objektyvių jo taikymo įrodymų.

1 – pradinis lygis. Atskiros priemonės taikomos fragmentiškai ir daugiausia reaktyviai; procesai nėra pakankamai formalizuoti, o atsakomybės nėra aiškiai apibrėžtos.

2 – apibrėžtas lygis. Pagrindiniai procesai ir atsakomybės yra apibrėžti bei dokumentuoti, tačiau jų praktinis taikymas nėra visiškai nuoseklus arba integruotas į bendrą organizacijos valdymą.

3 – valdomas lygis. Procesai taikomi sistemingai, jų vykdymas stebimas ir vertinamas, nustatytos atsakomybės, o gauti rezultatai naudojami valdymo sprendimams priimti.

4 – optimizuojamas lygis. Procesai nuolat vertinami ir tobulinami remiantis veiklos rodikliais, rizikų pokyčiais, incidentų analize, auditų rezultatais ir organizaciniu mokymusi.

37 lentelė. Kibernetinio saugumo valdymo brandos vertinimo matrica

Kodas	Vertinimo sritis ir kriterijus	Galimi vertinimo įrodymai	Balas (0–4)	Tobulinimo poreikis / planuojami veiksmai
D1. Strateginė integracija				
D1.1	Kibernetinis saugumas įtrauktas į organizacijos strateginius tikslus ir veiklos planus	Strategija, veiklos planai, kibernetinio saugumo politika		
D1.2	Vadovybė periodiškai dalyvauja vertinant kibernetinio saugumo rizikas, incidentus ir prioritetus	Vadovybės posėdžių protokolai, ataskaitos, rizikų peržiūros		
D1.3	Kibernetinio saugumo sprendimai siejami su organizacijos veiklos tęstinumo, pacientų saugos ir e. sveikatos paslaugų patikimumo tikslais	Strateginiai dokumentai, veiklos tęstinumo ir rizikų valdymo dokumentai		
D2. Atsakomybės ir koordinavimas				
D2.1	Aiškiai nustatytos kibernetinio saugumo funkcijos ir atsakomybės	Pareigybių aprašymai, atsakomybių matrica, vidaus teisės aktai		
D2.2	Strateginio, taktinio, operacinio ir technologinio valdymo lygmenų atsakomybės tarpusavyje suderintos	Organizacinė struktūra, procesų aprašai, atsakomybių schema		
D2.3	Nustatyti padalinių ir, kai aktualu, išorinių subjektų koordinavimo bei informacijos apsikeitimo mechanizmai	Bendradarbiavimo procedūros, sutartys, kontaktų ir eskalavimo schemos		
D3. Rizikų valdymo branda				
D3.1	Kibernetinės rizikos identifikuojamos ir periodiškai vertinamos	Rizikų registras, rizikos vertinimo ataskaitos		
D3.2	Rizikų vertinimas apima technologines, organizacines, duomenų apsaugos, tiekimo grandinės ir e. sveikatos paslaugų tęstinumo rizikas	Rizikų vertinimo metodika ir registras		
D3.3	Rizikų vertinimo rezultatai naudojami nustatant saugumo prioritetus, priemones ir išteklių poreikį	Rizikų valdymo planai, veiksmų planai, investicijų pagrindimas		

Kodas	Vertinimo sritis ir kriterijus	Galimi vertinimo įrodymai	Balas (0–4)	Tobulinimo poreikis / planuojami veiksmai
D4. Incidentų valdymas ir organizacinis mokymasis				
D4.1	Veikia formalizuotas kibernetinių incidentų registravimo, klasifikavimo ir eskalavimo procesas	Incidentų valdymo procedūra, incidentų registras		
D4.2	Apibrėžti reagavimo, komunikavimo, atkūrimo ir atsakingų asmenų veiksmai incidento metu	Incidentų valdymo planas, eskalavimo schema, kontaktų sąrašai		
D4.3	Po reikšmingų incidentų atliekama priežasčių ir pasekmių analizė, o nustatytos pamokos panaudojamos procesams tobulinti	Incidentų analizės ataskaitos, korekcinių veiksmų planai		
D5. Duomenų apsauga ir privatumas				
D5.1	Sveikatos duomenų tvarkymo procesai grindžiami konfidencialumo, vientisumo, prieinamumo ir atsekamumo principais	Duomenų apsaugos politika, saugumo dokumentai, auditų rezultatai		
D5.2	Nustatytos techninės ir organizacinės sveikatos duomenų apsaugos priemonės	Šifravimo, prieigos kontrolės, žurnalų ir kitų priemonių dokumentacija		
D5.3	Duomenų apsaugos ir kibernetinio saugumo reikalavimai integruojami į naujų ar keičiamų e. sveikatos sprendimų kūrimą ir diegimą	Projektų dokumentacija, rizikos ir poveikio vertinimai, saugumo reikalavimai		
D6. Technologinė architektūra ir stebėsena				
D6.1	Technologinės saugumo priemonės sudaro tarpusavyje suderintą saugumo architektūrą	Architektūros schemos, saugumo sprendimų dokumentacija		
D6.2	Vykdoma saugumo įvykių ir žurnalinių įrašų stebėsena bei analizė	SIEM ar kitų stebėsenos sistemų duomenys, žurnalų analizės procedūros		
D6.3	Sistemingai valdomi pažeidžiamumai, saugumo atnaujinimai ir technologinės rizikos	Pažeidžiamumų skenavimo rezultatai, atnaujinimų registrai, veiksmų planai		

Kodas	Vertinimo sritis ir kriterijus	Galimi vertinimo įrodymai	Balas (0–4)	Tobulinimo poreikis / planuojami veiksmai
D6.4	Vertinamas e. sveikatos sistemų, integracijų ir, kai taikoma, medicininių prietaisų kibernetinis saugumas	Techninių vertinimų ir auditų rezultatai, inventorizacijos duomenys		
D7. Tapatybių ir prieigų valdymas				
D7.1	Naudotojų prieigos suteikiamos pagal nustatytus vaidmenis ir realų veiklos poreikį	Prieigų valdymo politika, naudotojų teisių matrica		
D7.2	Privilegijuotos prieigos yra atskirai kontroliuojamos ir periodiškai peržiūrimos	Privilegijuotų paskyrų sąrašai, peržiūrų rezultatai		
D7.3	Kritinėms sistemoms ir prieigoms taikomas daugiafaktoris tapatybės patvirtinimas, kai tai techniškai ir organizaciškai taikytina	MFA konfigūracijos, autentifikavimo politika		
D7.4	Darbo santykių ar funkcijų pasikeitimo atveju naudotojų teisės laiku keičiamos arba panaikinamos	Naudotojų teisių peržiūros, personalo ir IT procesų įrašai		
D8. Saugumo kultūra ir darbuotojų kompetencijos				
D8.1	Darbuotojams periodiškai organizuojami kibernetinio saugumo mokymai	Mokymų planai, dalyvių sąrašai, mokymo medžiaga		
D8.2	Mokymų turinys siejamas su darbuotojų funkcijomis ir organizacijai aktualiomis grėsmėmis	Diferencijuotos mokymo programos, mokymų temos		
D8.3	Darbuotojų pasirengimas vertinamas praktiniais testais, pratybomis ar kitomis patikrinimo priemonėmis	Socialinės inžinerijos testai, pratybų rezultatai, žinių patikrinimai		
D8.4	Vadovybė ir padalinių vadovai savo sprendimais palaiko kibernetinio saugumo kultūrą	Vidaus komunikacija, vadovybės iniciatyvos, veiklos planai		
D9. Veiklos tęstinumas ir kibernetinis atsparumas				
D9.1	Nustatytos kritinės e. sveikatos paslaugos ir jų atkūrimo prioritetai	Veiklos poveikio analizė, tęstinumo planai		

Kodas	Vertinimo sritis ir kriterijus	Galimi vertinimo įrodymai	Balas (0–4)	Tobulinimo poreikis / planuojami veiksmai
D9.2	Parengti ir periodiškai atnaujinami veiklos tęstinumo ir atkūrimo planai	Tęstinumo, atkūrimo ir krizių valdymo planai		
D9.3	Atsarginės kopijos periodiškai testuojamos, o atkūrimo galimybės praktiškai tikrinamos	Atsarginių kopijų ir atkūrimo testų rezultatai		
D9.4	Periodiškai vykdomos incidentų, veiklos tęstinumo arba kibernetinių krizių pratybos	Pratybų scenarijai, ataskaitos, nustatyti korekciniai veiksmai		
D9.5	Tęstinumo ir atsparumo vertinimo rezultatai naudojami tolesniam procesų ir saugumo priemonių tobulinimui	Vadovybės peržiūros, veiksmų planai, pakartotinių vertinimų rezultatai		

Šaltinis: sudaryta autorės, remiantis disertacijoje sukurtu ir ekspertinio tyrimo pagrindu patikslintu kibernetinio saugumo valdymo modeliu.

Kiekvienos vertinimo dimensijos brandos indeksas apskaičiuojamas kaip tai dimensijai priskirtų kriterijų balų aritmetinis vidurkis:

$$BI_d = \frac{\sum_{i=1}^{n_d} x_i}{n_d}$$

BI_d – vertinamos dimensijos brandos indeksas;
x_i – konkrečiam dimensijos kriterijui suteiktas balas;
n_d – konkrečiai dimensijai priskirtų vertinimo kriterijų skaičius.

Bendras organizacijos kibernetinio saugumo valdymo brandos indeksas apskaičiuojamas pagal visų vertinimo kriterijų rezultatus:

$$KSB = \frac{\sum_{i=1}^{n} x_i}{n}$$

KSB – bendras kibernetinio saugumo valdymo brandos indeksas;
x_i – atskiram vertinimo kriterijui priskirtas balas nuo 0 iki 4;
n – visų vertinamų kriterijų skaičius.

Visiems kriterijams suteikiamas vienodas svoris. Toks skaičiavimo principas pasirinktas siekiant išlaikyti metodikos aiškumą ir vertinimo rezultatų palyginamumą bei išvengti subjektyvumo, kuris galėtų atsirasti skirtingoms kriterijų grupėms priskiriant nevienodus svorius.

38 lentelė. Bendro brandos indekso interpretavimas

Brandos indeksas	Brandos lygis	Rezultato interpretavimas
0,00–0,79	Neįgyvendinta	Kibernetinio saugumo valdymo praktikos iš esmės nėra įgyvendintos arba jų taikymo negalima pagrįsti pakankamais įrodymais.
0,80–1,59	Pradinis	Atskiros priemonės taikomos, tačiau valdymas išlieka fragmentiškas, daugiausia reaktyvus ir nepakankamai formalizuotas.
1,60–2,39	Apibrėžtas	Pagrindiniai procesai ir atsakomybės yra nustatyti, tačiau jų praktinis taikymas dar nėra visiškai nuoseklus ir integruotas.
2,40–3,19	Valdomas	Procesai taikomi sistemingai, stebimi ir vertinami, o vertinimo rezultatai naudojami priimant valdymo sprendimus.
3,20–4,00	Optimizuojamas	Kibernetinio saugumo valdymas integruotas į organizacijos veiklą, o procesų tobulinimas grindžiamas duomenimis, rizikų pokyčiais, incidentų ir auditų rezultatais bei organizaciniu mokymusi.

Šaltinis: sudaryta autorės

Brandos indeksas parodo kibernetinio saugumo valdymo procesų išvystymo lygį, tačiau vien jo nepakanka praktiniam modelio taikymo rezultatui įvertinti. Dėl šios priežasties periodinį brandos vertinimą tikslinga papildyti operacinių kibernetinio atsparumo rodiklių stebėsena. Šių rodiklių reikšmės turėtų būti fiksuojamos atliekant pradinį vertinimą ir lyginamos su vėlesnių vertinimų rezultatais.

39 lentelė. Operacinių rodiklių sąrašas

Vertinama sritis	Galimas rodiklis	Vertinimo paskirtis	Pradinė reikšmė	Pakartotinio vertinimo reikšmė
Pasirengimas	Atliktų kibernetinio saugumo pratybų skaičius per metus	Vertinti organizacijos pasirengimo incidentams aktyvumą		
Pasirengimas	Sėkmingai atliktų atsarginių kopijų atkūrimo testų dalis	Vertinti realų pasirengimą atkurti sistemas ir duomenis		
Aptikimas	Vidutinis incidento aptikimo laikas	Vertinti organizacijos gebėjimą laiku nustatyti incidentą		

Vertinama sritis	Galimas rodiklis	Vertinimo paskirtis	Pradinė reikšmė	Pakartotinio vertinimo reikšmė
Reagavimas	Vidutinis reagavimo į incidentą laikas	Vertinti reagavimo proceso operatyvumą		
Atkūrimas	Vidutinė kritinės paslaugos atkūrimo trukmė	Vertinti gebėjimą atkurti veiklą po sutrikimo		
Paslaugų tęstinumas	Kritinių e. sveikatos paslaugų prieinamumas	Vertinti kritinių paslaugų tęstinumą		
Incidentų valdymas	Užregistruotų incidentų, kuriems atlikta analizė po incidento, dalis	Vertinti organizacinio mokymosi nuoseklumą		
Tobulinimas	Laiku įgyvendintų korekcinių veiksmų dalis	Vertinti nustatytų trūkumų šalinimo veiksmingumą		
Darbuotojų kompetencijos	Kibernetinio saugumo mokymus baigusių darbuotojų dalis	Vertinti darbuotojų įtrauktį į saugumo kompetencijų stiprinimą		
Valdymo branda	Bendro kibernetinio saugumo valdymo brandos indekso pokytis	Vertinti organizacijos valdymo brandos raidą		

Šaltinis: sudaryta autorės, remiantis disertacijoje išskirtomis kibernetinio atsparumo operacinėmis dimensijomis ir rodikliais.

Operacinių rodiklių sąrašas nėra baigtinis. Konkreti organizacija jį gali adaptuoti atsižvelgdama į savo dydį, informacinių sistemų architektūrą, teikiamų paslaugų kritiškumą, turimus stebėsenos duomenis ir kibernetinio saugumo brandą. Svarbu išlaikyti tuos pačius rodiklių apskaičiavimo principus skirtingais vertinimo laikotarpiais, kad jų reikšmės būtų palyginamos.

Atlikus vertinimą pirmiausia analizuojamas bendras kibernetinio saugumo valdymo brandos indeksas, tačiau praktiniam valdymo tobulinimui svarbesnė yra atskirų dimensijų rezultatų analizė. Žemesnį brandos įvertį gavusios sritys parodo, kuriose modelio dalyse yra didžiausias atotrūkis tarp siekiamos ir esamos valdymo būklės.

Vertinimo rezultatai gali būti naudojami rengiant kibernetinio saugumo tobulinimo planą, nustatant prioritetinius veiksmus, planuojant išteklius ir stebint pažangą. Kriterijai, įvertinti 0 arba 1 balu, turėtų būti vertinami kaip prioritetinės tobulinimo sritys. 2 balais įvertintose srityse pagrindinis dėmesys turėtų būti skiriamas jau nustatytų procesų nuosekliam įgyvendinimui ir integravimui į bendrą organizacijos valdymą. 3 ar 4 balų įvertinimas rodo labiau išvystytą valdymo praktiką, tačiau tokiose srityse taip pat svarbu užtikrinti periodinę stebėseną ir nuolatinį tobulinimą.

Pakartotinį vertinimą rekomenduojama atlikti periodiškai arba po reikšmingų

organizacinių, technologinių ar reguliacinių pokyčių. Lyginant bendro brandos indekso, atskirų dimensijų ir pasirinktų operacinių rodiklių reikšmes skirtingais laikotarpiais, galima stebėti kibernetinio saugumo valdymo raidą ir vertinti, ar įgyvendinti tobulinimo veiksmai siejasi su teigiamais organizacijos pasirengimo, incidentų valdymo, atkūrimo ir veiklos tęstinumo pokyčiais.

Ši metodika nėra skirta formaliam organizacijų sertifikavimui ar universaliam jų tarpusavio reitingavimui. Jos paskirtis – sudaryti nuoseklų ir praktiškai taikomą pagrindą konkrečios e. sveikatos organizacijos kibernetinio saugumo valdymo būklei įvertinti, tobulinimo prioritetams nustatyti ir pokyčiams stebėti taikant disertacijoje siūlomą kibernetinio saugumo valdymo modelį.

MYKOLO ROMERIO UNIVERSITETAS

Lina Lelešienė

KIBERNETINIO SAUGUMO VALDYMO MODELIO E. SVEIKATOS SISTEMOS TOBULINIMUI VERTINIMAS

Mokslo daktaro disertacijos santrauka
Socialiniai mokslai, vadyba (S 003)

Vilnius, 2026

Mokslo daktaro disertacija rengta 2020–2026 metais Mykolo Romerio universitete pagal Vytauto Didžiojo universitetui su Klaipėdos universitetu, Mykolo Romerio universitetu ir Vilniaus universitetu Lietuvos Respublikos švietimo, mokslo ir sporto ministro 2019 m. vasario 22 d. įsakymu Nr. V-160 suteiktą doktorantūros teisę.

Mokslinis vadovas:
prof. dr. Tadas Limba (Mykolo Romerio universitetas, socialiniai mokslai, vadyba, S 003).

Mokslo daktaro disertacija ginama Vytauto Didžiojo universiteto, Klaipėdos universiteto, Mykolo Romerio universiteto ir Vilniaus universiteto Šiaulių akademijos vadybos mokslo krypties taryboje:

Pirmininkas:
prof. dr. Andrius Stasiukynas (Mykolo Romerio universitetas, socialiniai mokslai, vadyba, S 003).

Nariai:
prof. dr. Vida Davidavičienė (Vilniaus Gedimino technikos universitetas, socialiniai mokslai, vadyba, S 003);
prof. dr. Iveta Reinholde (Latvijos universitetas, Latvijos Respublika, socialiniai mokslai, politikos mokslai, S 002);
prof. dr. Rimantas Stašys (Klaipėdos universitetas, socialiniai mokslai, vadyba, S 003);
prof. dr. Jolita Vveinhardt (Vytauto Didžiojo universitetas, socialiniai mokslai, vadyba, S 003).

Mokslo daktaro disertacija bus ginama viešame Vadybos mokslo krypties tarybos posėdyje 2026 m. lapkričio 10 d. 10 val. Mykolo Romerio universitete, I-414 auditorijoje.
Adresas: Ateities g. 20, 08303 Vilnius.

© Mykolo Romerio universitetas, 2026

SANTRAUKA

Temos aktualumas. E. sveikatos sistemos plėtra iš esmės keičia sveikatos priežiūros paslaugų organizavimą ir duomenų valdymą. Vis daugiau sveikatos priežiūros procesų vyksta skaitmeninėje aplinkoje – nuo elektroninių sveikatos įrašų ir e. recepto iki pacientų registracijos, medicininių dokumentų mainų bei duomenų perdavimo tarp sveikatos priežiūros įstaigų. Tokie sprendimai padeda greičiau keistis informacija, efektyviau organizuoti paslaugas ir sudaro patogesnes sąlygas tiek pacientams, tiek sveikatos priežiūros specialistams.

Kartu didėjanti skaitmenizacija sukuria ir naujų kibernetinio saugumo iššūkių. E. sveikatos sistemoje tvarkomi itin jautrūs asmens sveikatos duomenys, o skirtingų informacinių sistemų tarpusavio sąveika reiškia, kad saugumo pažeidimas vienoje grandyje gali paveikti ir kitus sistemos dalyvius. Duomenų nutekinimas, neautorizuota prieiga, e. recepto, pacientų portalo ar medicininių dokumentų mainų sutrikimai gali turėti pasekmių ne tik duomenų apsaugai, bet ir paslaugų tęstinumui bei pacientų pasitikėjimui. Todėl e. sveikatos kibernetinis saugumas turi būti suprantamas ne vien kaip techninių apsaugos priemonių taikymas, bet kaip nuoseklus valdymo procesas, apimantis rizikų vertinimą, atsakomybių paskirstymą, incidentų valdymą, duomenų apsaugą ir nuolatinį sistemos tobulinimą.

Pastaraisiais metais sveikatos sektorius vis dažniau įvardijamas kaip vienas iš pažeidžiamiausių kibernetinių atakų taikinių, nes jame susikerta jautrių duomenų apsauga, kritinių paslaugų tęstinumas ir riboti organizaciniai ištekliai. Tai rodo, kad vien pavienėmis techninėmis priemonėmis grįstas saugumo valdymas nėra pakankamas. Sveikatos priežiūros įstaigos tampa ypač patraukliu taikiniu dėl jų valdomų ypač jautrių duomenų, kritinės infrastruktūros statuso ir dažnai ribotų išteklių pažangioms saugumo priemonėms diegti. Išpirkos reikalaujančios (*angl. ransomware*) atakos, asmens duomenų saugumo pažeidimai, paslaugų trikdymai, neautorizuotos prieigos prie e. sveikatos informacinių sistemų ar tinkle veikiančių medicininių prietaisų atvejai kelia riziką ne tik asmens duomenų apsaugai, bet ir sveikatos paslaugų tęstinumui, o tai gali tiesiogiai paveikti pacientų saugumą. Dėl šios priežasties šiame darbe kibernetinio saugumo valdymas nagrinėjamas ne kaip pavienių techninių priemonių rinkinys, o kaip nuoseklus valdymo procesas, pritaikytas e. sveikatos sistemos struktūrai ir jos veikimo specifikai. Reglamentavimo lygmeniu kibernetinio saugumo svarba nuosekliai didėja, o teisės aktai (tokie dokumentai kaip TIS2 direktyva, BDAR, ISO/IEC 27001, ISO/IEC 27005:2018, ISO/IEC 27035-1:2023, ISO/IEC 27701:2019 ir ISO/IEC 27032:2023) įtvirtina griežtesnius informacijos saugumo ir rizikų valdymo reikalavimus, akcentuoja poreikį sistemingam informacijos saugumo valdymui, rizikos vertinimo procesų integracijai ir nuolatiniam organizacijų saugumo brandos didinimui. Vis dėlto praktikoje sveikatos sektoriaus organizacijos dažnai susiduria su iššūkiais perkeliant šiuos standartus į realius vadybinius sprendimus. Dėl to šiame darbe pagrindžiamas poreikis formuoti tokį kibernetinio saugumo valdymo modelį, kuris sujungtų tarptautinių standartų nuostatas, nacionalinį reguliavimą ir e. sveikatos sistemos organizacinę bei technologinę specifiką.

Temos aktualumą stiprina ir organizaciniai veiksniai. Sveikatos priežiūros įstaigų gebėjimas valdyti kibernetinį saugumą priklauso ne tik nuo technologijų, bet ir nuo darbuotojų kompetencijų, atsakomybių paskirstymo, vidinių procedūrų ir vadovybės įsitraukimo. Empiriniai tyrimai rodo, kad kibernetinio saugumo kultūra, darbuotojų žinios ir įgūdžiai, aiškiai apibrėžti valdymo procesai bei organizacinės struktūros veiksmingumas lemia, kaip efektyviai sveikatos sektoriaus institucijos gali įgyvendinti saugumo priemones ir reaguoti į kylančias grėsmes. Tačiau sveikatos sektoriuje vis dar trūksta empirinių modelių, leidžiančių įvertinti ir palyginti kibernetinio saugumo valdymo brandą skirtinguose e. sveikatos sistemos lygmenyse. Todėl mokslinis indėlis, kuriant ir vertinant kibernetinio saugumo valdymo modelį, gali turėti reikšmingą praktinę vertę, didinant sprendimų priėmimo efektyvumą, išteklių paskirstymo racionalumą ir organizacijų atsparumą kibernetinėms grėsmėms.

Šioje disertacijoje e. sveikatos sistemos kibernetinio saugumo valdymas traktuojamas kaip mokslinė ir praktinė problema, kylanti iš e. sveikatos infrastruktūros kompleksiškumo, didėjančių kibernetinių rizikų ir poreikio valdymo sprendimus susieti su konkrečia e. sveikatos sistemos struktūra.

Nors informacijos saugumo valdymas plačiai nagrinėjamas ekonomikos ir vadybos srityse, esamų žinių nepakanka kuriant kibernetinio saugumo valdymo modelius, pritaikomus e. sveikatos sistemoms. Mokslininkai pabrėžia, kad kritinės infrastruktūros apsauga reikalauja kompleksinio požiūrio, o e. sveikatos sistema yra viena svarbiausių sveikatos sektoriaus inovacijų, kuri pasižymi dideliu duomenų jautrumu ir procesų sudėtingumu. Nors jos ekonominė, socialinė ir organizacinė nauda yra akivaizdi, sukurti vertės vertinimą leidžiančius metodus vis dar sudėtinga. Praktikoje taikomi įvairūs vertinimo modeliai padeda matuoti efektyvumą ir optimizuoti procesus, tačiau jų taikymas kinta priklausomai nuo sistemos tikslų, suinteresuotųjų šalių ir konteksto. Kadangi e. sveikatos paslaugos tiesiogiai susijusios su žmogaus sveikata ir jautriai vertinamos vartotojų, būtina turėti specialiai šiai sričiai pritaikytą kibernetinio saugumo valdymo modelį. Nepaisant šios srities aktualumo, kibernetinio saugumo valdymas e. sveikatos kontekste tarptautiniu mastu išlieka nepakankamai ištirtas.

Disertacijoje siekiama suformuoti kibernetinio saugumo valdymo modelį, kuris galėtų būti veiksmingai taikomas e. sveikatos sistemos kūrimo ir administravimo procesuose. Vienas iš ryškiausių iššūkių, su kuriais susiduria e. sveikatos infrastruktūra, yra nepakankamai užtikrinamas informacinių sistemų saugumas. Šiame darbe daroma prielaida, kad šioje disertacijoje kuriamas kibernetinio saugumo valdymo modelis gali sudaryti prielaidas nuoseklesnei ir spartesnei e. sveikatos sprendimų plėtrai. Šiuolaikinė technologinė raida lemia vis intensyvesnį jautrių duomenų perkėlimą į skaitmeninę aplinką, todėl kibernetinio saugumo problematika tampa vis aktualesnė tiek organizacijoms, tiek individualiems vartotojams. Didėjant priklausomybei nuo skaitmeninių paslaugų, auga ir pažeidžiamumas, o tai skatina tyrėjų ir visuomenės domėjimąsi šia sritimi. Norint veiksmingai valdyti kylančias rizikas, būtina kryptingai identifikuoti galimas grėsmes, vertinti jų poveikį ir numatyti prevencines priemones, užtikrinančias savalaikį jų suvaldymą.

Apibendrinus disertacijoje nagrinėtą mokslinę literatūrą, matyti keli probleminiai

aspektai, kylantys modeliuojant kibernetinio saugumo valdymo modelį e. sveikatos sistemų plėtros procese. Pirmiausia išryškėja sunkumai pasirenkant ir pritaikant tinkamiausius kibernetinio saugumo modelius, kurie galėtų būti taikomi kuriant ir tobulinant e. sveikatos infrastruktūrą. Taip pat pabrėžiama būtinybė aiškiai apibrėžti norimą rezultatą, nes tai lemia tinkamo valdymo modelio pasirinkimą ir jo pritaikymo logiką. Galiausiai, literatūroje akcentuojamas poreikis kurti vertinimo kriterijus, leidžiančius analizuoti ne atskirus sistemos elementus, bet visą e. sveikatos ekosistemą kaip vieningą darinį, taip sudarant galimybę integruoti skirtingus rodiklius į vientisą ir nuoseklų vertinimo pagrindą.

Taigi šioje disertacijoje kibernetinio saugumo valdymo modeliavimas analizuojamas kaip būdas sistemiškai susieti e. sveikatos infrastruktūros plėtrą, rizikų valdymą, incidentų valdymą, duomenų apsaugą ir atsparumo didinimo prielaidas.

Mokslinė problema – koks turi būti kibernetinio saugumo valdymo modelis, užtikrinantis veiksmingą e. sveikatos sistemos tobulinimą ir leidžiantis sumažinti kibernetinių grėsmių bei informacinių sistemų pažeidžiamumų rizikas?

Mokslinio tyrimo objektas – kibernetinio saugumo valdymo modelio vertinimas e. sveikatos sistemos kontekste.

Mokslinio tyrimo tikslas – parengti kibernetinio saugumo valdymo modelį e. sveikatos sistemos tobulinimui, sudarant prielaidas e. sveikatos sistemos atsparumui kibernetinėms grėsmėms didinti.

Tyrimo uždaviniai:

1. Išanalizuoti kibernetinio saugumo valdymo teorinius aspektus, principus ir esamus modelius, kibernetinio saugumo valdymo ypatumus e. sveikatos IS integracijos, duomenų apsaugos ir kibernetinio atsparumo kontekste.
2. Atlikti sisteminę e. sveikatos sistemų kibernetinių incidentų bei atakų analizę.
3. Parengti koncepcinį kibernetinio saugumo valdymo modelį, orientuotą į e. sveikatos sistemos projektavimo, diegimo, administravimo ir tobulinimo etapus.
4. Remiantis empirinio tyrimo ekspertų identifikuotomis problemomis ir gautais rezultatais, patikslinti sukurtą kibernetinio saugumo valdymo modelį e. sveikatos sistemos tobulinimui.
5. Ekspertiniu požiūriu įvertinti sukurto kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui tinkamumą, praktinį pritaikomumą, atitikimą sveikatos sektoriaus organizacijų praktikai ir galimus taikymo ribotumus.
6. Parengti rekomendacijas dėl patikslinto kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimo taikymo ir integravimo į e. sveikatos sistemos gerinimo procesus.

Mokslinio tyrimo metodai. Disertacijoje taikoma mokslinės literatūros, tarptautinių standartų ir teisės aktų lyginamoji analizė, siekiant identifikuoti kibernetinio saugumo valdymo principų, modelių ir metodikų taikymo kryptis, jų sąsajas bei skirtumus e. sveikatos sistemos kontekste. Teorinių šaltinių sisteminimas ir apibendrinimas leidžia išryškinti pagrindinius kibernetinių incidentų kilmės veiksnius, e. sveikatos infrastruktūros pažeidžiamumus, taip pat suformuoti pradinį konceptualų kibernetinio saugumo valdymo modelį, orientuotą į e. sveikatos sistemos projektavimo,

įgyvendinimo, administravimo ir tobulinimo procesus. Kai kurių mokslinių šaltinių ir citatų vertimui naudoti Europos Komisijos dirbtinio intelekto kalbos įrankiai.

Empirinėje tyrimo dalyje taikomas kokybinis tyrimo metodas – pusiau struktūruoti ekspertiniai interviu, kurių metu apklausiami kibernetinio saugumo valdymo, e. sveikatos sistemų administravimo, strateginio planavimo ir technologinių sprendimų diegimo srityse dirbantys specialistai. Ekspertų įžvalgos naudojamos pradinio modelio elementams tikslinti, įvertinti jų praktinį aktualumą, identifikuoti sistemines spragas ir suformuluoti modelio patobulinimus, atspindinčius realias e. sveikatos sistemos valdymo sąlygas.

Papildomai taikoma dokumentų analizė, leidžianti vertinti ekspertų pateiktas įžvalgas su normatyviniu reguliavimu, gairėmis, strateginiais dokumentais ir (kai aktualu) organizaciniais vidaus dokumentais. Interviu duomenys analizuojami taikant teminę analizę (*angl. thematic analysis*), sistemingai identifikuojant pasikartojančias temas, problemines sritis ir jų ryšius su modelio struktūriniais lygmenimis bei funkcinėmis dimensijomis. Remiantis teorinės analizės ir empirinio tyrimo rezultatais, atliekamas kibernetinio saugumo valdymo modelio koregavimas ir patobulinimas, o darbo pabaigoje formuluojamos apibendrintos mokslinės ir praktinės išvados bei rekomendacijos dėl modelio taikymo e. sveikatos sistemos tobulinimo procesuose.

Disertacijos ginamieji teiginiai:

1. E. sveikatos kibernetinio saugumo valdymo veiksmingumas priklauso nuo jo integravimo į bendrą organizacijos valdymą, vadovybės įsitraukimo ir aiškaus atsakomybių paskirstymo.
2. Kibernetinio saugumo valdymo fragmentiškumą mažina nuosekli strateginio, taktinio, operacinio ir technologinio valdymo lygmenų sąveika.
3. Patikslintas kibernetinio saugumo valdymo modelis sudaro metodinį pagrindą valdymo spragoms nustatyti ir prioritetinėms tobulinimo kryptims pagrįsti.

Darbo naujumas ir praktinis reikšmingumas. Kibernetinio saugumo valdymas e. sveikatos sistemos kontekste yra tarpdisciplinė sritis, kurioje susikerta informacinių technologijų, vadybos, teisės, viešojo administravimo ir sveikatos mokslų problematika. Nors pasaulyje atliekama nemažai tyrimų, nagrinėjančių kibernetinio saugumo klausimus, dauguma jų analizuoja šį reiškinį tik vienos mokslo krypties rėmuose, neatsižvelgdami į platesnį organizacinių, procesinių ir reguliacinių veiksnių kontekstą. Dėl šios priežasties kibernetinis saugumas dažnai traktuojamas fragmentiškai – kaip technologinis iššūkis arba kaip teisinės atitikties problema, nors veiksmingas saugumo užtikrinimas reikalauja integruoto, kelių mokslo sričių žiniomis grindžiamo požiūrio.

Šio disertacinio darbo naujumas pasireiškia tuo, kad kibernetinio saugumo valdymas tiriamas kompleksiškai, jungiant technologinius, organizacinius, procesinius ir teisinius e. sveikatos sistemos aspektus. Atlikus mokslinės literatūros, tarptautinių standartų ir praktinių e. sveikatos sistemų atvejų analizę, disertacijoje identifikuojami specifiniai kibernetinio saugumo valdymo pažeidžiamumai, rizikos veiksniai ir e. sveikatos infrastruktūros sąveikos trūkumai, turintys esminės įtakos sistemos patikimumui. Tyrimo metu taip pat analizuojamos tarptautinės e. sveikatos sistemų kibernetinių incidentų praktikos, leidžiančios įvertinti tarptautiniuose tyrimuose ir praktikoje

išryškėjančias tendencijas ir išskirti ypač pažeidžiamus sistemos komponentus. Skirtingai nei egzistuojantys kibernetinio saugumo modeliai, šiame darbe siūlomas modelis integruoja strateginį, organizacinį, procesinį ir technologinį valdymo lygmenis būtent e. sveikatos sistemos ekosistemos kontekste ir yra empiriškai pagrįstas ekspertinio tyrimo duomenimis nacionaliniu kontekstu.

Darbo praktinis reikšmingumas atsiskleidžia keliais aspektais. Pirma, disertacijoje pateikiamas kibernetinio saugumo valdymo modelis gali būti tiesiogiai taikomas e. sveikatos sistemos tobulinimo, projektavimo ir administravimo procesuose, siekiant sudaryti prielaidas mažinti infrastruktūros pažeidžiamumą ir stiprinti sistemos atsparumą kibernetinėms grėsmėms. Antra, modelio vertinimo kriterijai ir struktūriniai elementai gali būti naudojami sveikatos priežiūros įstaigų vadovams ir politikos formuotojams priimant sprendimus dėl saugumo valdymo brandos didinimo, resursų paskirstymo ir rizikų mažinimo priemonių planavimui. Trečia, tyrimo rezultatai suteikia metodologinį pagrindą e. sveikatos politikos formavimui, standartų adaptavimui ir kibernetinio saugumo valdymo principų integravimui į strateginio valdymo dokumentus.

Disertacijoje siūlomas modelis gali būti taikomas ne tik e. sveikatos sistemos kūrimo ir eksploatavimo etapuose, bet ir atliekant periodinius e. sveikatos sistemos saugumo vertinimus, planuojant infrastruktūros modernizavimą bei stiprinant organizacijų pasirengimą reaguoti į kibernetines grėsmes. Tokiu būdu tyrimas prisideda prie e. sveikatos sistemos tvarios plėtros ir sudaro prielaidas saugesnių, patikimesnių ir visuomenės pasitikėjimą užtikrinančių e. sveikatos paslaugų plėtojimui Lietuvoje.

Darbo struktūra.

Disertacinį darbą sudaro trys tarpusavyje logiškai susijusios dalys.

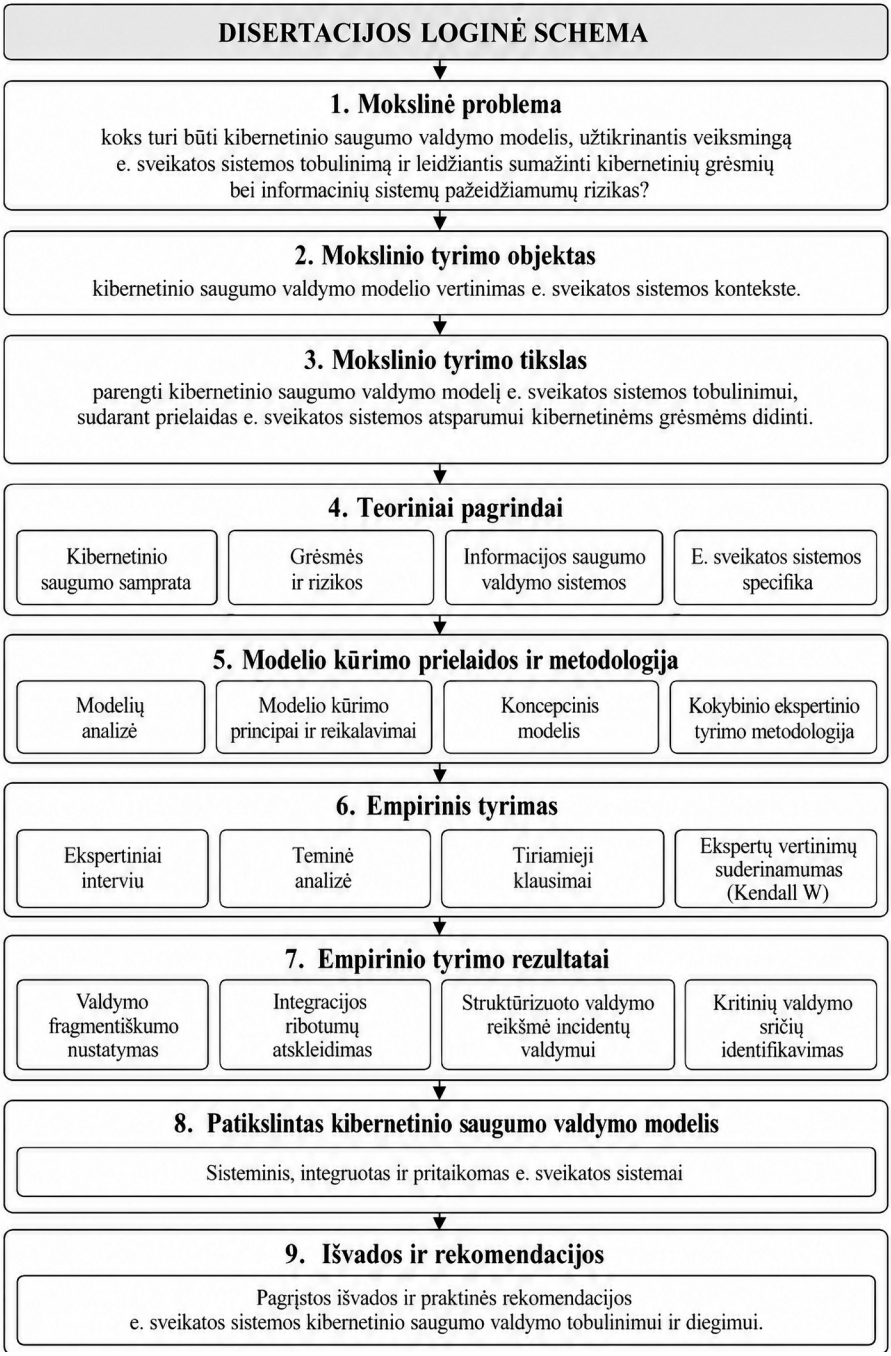
Pirmojoje disertacijos dalyje nagrinėjami kibernetinio saugumo valdymo teoriniai aspektai. Joje analizuojama kibernetinio saugumo sampratos raida, pagrindiniai principai ir tikslai, aptariamos šiuolaikinės kibernetinės grėsmės ir rizikos, ypač aktualios e. sveikatos sektoriui. Taip pat nagrinėjamos informacijos saugumo valdymo sistemos, tarptautiniai standartai (ISO/IEC 27001, 27005), TIS2 direktyvos reikalavimai bei kibernetinio saugumo brandos modeliai. Pirmoji dalis sudaro teorinį pagrindą tolesnei modelio kūrimo ir empirinio vertinimo analizei.

Antrojoje disertacijos dalyje pateikiama kibernetinio saugumo valdymo modelio e. sveikatos sistemos tobulinimui struktūros kūrimo koncepcija ir tyrimo metodologinis pagrindimas. Šioje dalyje analizuojami egzistuojantys teoriniai ir praktiniai kibernetinio saugumo valdymo modeliai, formuluojami modelio kūrimo principai ir reikalavimai, apibrėžiamos prielaidos modelio struktūrai, valdymo lygiai, informacijos srautai ir atsakomybės paskirstymas. Taip pat detaliai pagrindžiama tyrimo metodologija, aprašomas tyrimo dizainas, ekspertų atranka, duomenų rinkimo priemonės bei taikyti duomenų analizės metodai.

Trečiojoje disertacijos dalyje pateikiami empirinio tyrimo rezultatai ir jų analizė. Šioje dalyje, remiantis ekspertinio interviu duomenimis, vertinamas kibernetinio saugumo valdymo lygis sveikatos įstaigose, identifikuojamos esminės kibernetinio saugumo spragos, analizuojamos rizikų ir incidentų valdymo praktikos bei atliekama teminė

ekspertinių įžvalgų analizė. Gauti empiriniai rezultatai naudojami kritinių kibernetinio saugumo valdymo sričių identifikavimui ir siūlomo valdymo modelio tikslinimui. Atliekamas siūlomo kibernetinio saugumo valdymo modelio ekspertinis vertinimas. Joje analizuojamas modelio tinkamumas ir taikymo galimybės e. sveikatos sistemoje, įvertinamos modelio stiprybės ir ribotumai, suformuluojamos pagrįstos tobulinimo kryptys bei aptariamas modelio praktinis pritaikomumas skirtinguose organizaciniuose ir instituciniuose kontekstuose.

Darbo pabaigoje pateikiamos apibendrintos disertacijos išvados ir rekomendacijos, kuriose sistemiškai apžvelgiami pagrindiniai tyrimo rezultatai, įvertinamas pasiektas tyrimo tikslas ir suformuluojamos praktinės bei mokslinės rekomendacijos e. sveikatos sistemos kibernetinio saugumo valdymo tobulinimui (žr. 1 pav.).



1 pav. Disertacinio darbo struktūros loginė schema.

Šaltinis: sudaryta autorės

PIRMOSIOS DALIES APŽVALGA: KIBERNETINIO SAUGUMO VALDYMO TEORINIAI ASPEKTAI

Pirmojoje disertacijos dalyje suformuotas teorinis ir konceptualus pagrindas, reikalingas kibernetinio saugumo valdymo modeliui e. sveikatos sistemos kontekste pagrįsti ir tolesniam empiriniam tyrimui atlikti. Šioje dalyje analizuojama kibernetinio saugumo samprata, jo reikšmė skaitmenizuotoje aplinkoje ir specifiniai iššūkiai, kylantys kritiniuose sektoriuose, ypatingą dėmesį skiriant sveikatos sistemai.

Kibernetinio saugumo sampratos raidos analizė parodė, kad šiuolaikiniame kontekste kibernetinis saugumas negali būti suprantamas vien kaip techninių apsaugos priemonių visuma. Mokslinėje literatūroje ir tarptautiniuose reguliaciniuose dokumentuose jis vis dažniau siejamas su organizacijų gebėjimu valdyti rizikas, užtikrinti veiklos tęstinumą ir prisitaikyti prie kintančios grėsmių aplinkos. Toks požiūris apima technologinius, organizacinius, teisinius ir žmogiškuosius aspektus ir pagrindžia disertacijoje taikomą nuostatą, kad kibernetinis saugumas turi būti integruojamas į bendrą organizacijos valdymo sistemą, o ne paliekamas vien informacinių technologijų padalinių atsakomybei.

Kibernetinių grėsmių, rizikų ir incidentų analizė atskleidė, kad šiuolaikinės grėsmės pasižymi dinamiškumu ir kompleksiškumu, o jų poveikį lemia ne tik techniniai pažeidžiamumai, bet ir organizacinės, procesinės bei žmogiškosios spragos. Kibernetinių incidentų klasifikavimo požiūrių analizė parodė, kad vien techniniai klasifikavimo modeliai nėra pakankami vertinant incidentų poveikį sudėtingoms socio-techninėms sistemoms. E. sveikatos sektoriuje ypač reikšmingos daugiamatės klasifikacijos, apimančios technologinius, organizacinius, klinikinius ir veiklos tęstinumo aspektus, nes kibernetiniai incidentai gali paveikti ne tik informacijos saugumą, bet ir paslaugų prieinamumą, pacientų saugą bei sveikatos duomenų patikimumą.

E. sveikatos sektoriaus rizikos veiksnių analizė parodė, kad kibernetinės rizikos formuojasi dėl tarpusavyje susijusių technologinių, organizacinių, reguliacinių ir žmogiškųjų veiksnių. Informacinių sistemų integracija, medicininių įrenginių prijungimas prie tinklų, didelis sveikatos duomenų jautrumas, paslaugų tęstinumo reikalavimai ir fragmentuotos valdymo struktūros sukuria aplinką, kurioje bendro pobūdžio rizikų valdymo modelių nepakanka. Dėl to pagrįstas poreikis formuoti kibernetinio saugumo valdymo modelį, pritaikytą e. sveikatos sistemos struktūrai, jos veikimo logikai, tarpinstitucinėms sąsajoms ir organizacinėms atsakomybėms.

Pirmojoje dalyje taip pat išanalizuotos informacijos saugumo valdymo sistemos, tarptautiniai standartai, įskaitant ISO/IEC 27001 ir ISO/IEC 27005, bei Europos Sąjungos kibernetinio saugumo reguliavimo pagrindai, tarp jų – TIS2 direktyva. Analizė parodė, kad standartai ir reguliaciniai reikalavimai sudaro reikšmingą metodinį kibernetinio saugumo pagrindą, tačiau vien jų nepakanka nuosekliam saugumo valdymui užtikrinti. Praktikoje jų įgyvendinimą riboja formalizavimas, valdymo fragmentiškumas ir nepakankamas saugumo reikalavimų susiejimas su organizacijos sprendimų priėmimo procesais. Todėl reguliacinė atitiktis disertacijoje vertinama ne kaip savarankiška administracinė funkcija, bet kaip viena iš integruotos kibernetinio saugumo

valdymo sistemos dimensijų.

Sveikatos sektoriaus kibernetinio saugumo valdymo analizė atskleidė didelį e. sveikatos sistemos struktūrinį ir funkcinį sudėtingumą. Informacinių sistemų sąveika, intensyvūs duomenų mainai, skirtingų institucijų dalyvavimas, medicininių prietaisų integracija ir aukšti paslaugų prieinamumo reikalavimai lemia poreikį kibernetinį saugumą valdyti sistemiškai. Vadybiniu požiūriu tai reiškia strateginio planavimo, aiškaus atsakomybių paskirstymo, rizikų ir incidentų valdymo, tarpinstitucinio koordinavimo, technologinių kontrolės priemonių, duomenų apsaugos, veiklos tęstinumo ir brandos vertinimo tarpusavio susiejimą.

Apibendrinant galima teigti, kad pirmojoje disertacijos dalyje suformuotas teorinis pagrindas leidžia pereiti nuo bendrųjų kibernetinio saugumo sampratų prie e. sveikatos sistemai pritaikyto valdymo modelio kūrimo. Identifikuoti grėsmių, rizikų, incidentų ir valdymo spragų dėsningumai pagrindžia poreikį kibernetinį saugumą e. sveikatos sistemoje vertinti kaip integruotą vadybinį procesą. Šios įžvalgos sudaro loginį pagrindą antrajai disertacijos daliai, kurioje analizuojami kibernetinio saugumo valdymo modeliai, formuluojamos modelio kūrimo prielaidos ir pagrindžiama empirinio tyrimo metodologija.

ANTROSIOS DALIES APŽVALGA: KIBERNETINIO SAUGUMO VALDYMO MODELIO E. SVEIKATOS SISTEMOS TOBULINIMUI STRUKTŪROS KŪRIMAS IR TYRIMO METODOLOGIJA

Antrojoje disertacijos dalyje pereinama nuo teorinių kibernetinio saugumo sampratų ir problematikos analizės prie kibernetinio saugumo valdymo modelio, skirto e. sveikatos sistemos kontekstui, formavimo ir empirinio tyrimo metodologinio pagrindimo. Ši dalis atlieka jungiamąją funkciją – joje pirmojoje dalyje suformuotos teorinės įžvalgos susiejamos su modelio kūrimo prielaidomis, jo struktūrine logika ir empiriniu vertinimu.

Pirmiausia atlikta sisteminė kibernetinio saugumo valdymo modelių analizė, apimanti teorinius ir praktikoje taikomus požiūrius įvairiuose sektoriuose, įskaitant sveikatos sektorių ir kritinės infrastruktūros sritis. Analizė parodė, kad esami modeliai suteikia reikšmingą metodinį pagrindą kibernetinio saugumo procesams struktūruoti, rizikoms valdyti ir organizacijų brandai vertinti, tačiau jų tiesioginis pritaikymas e. sveikatos sistemos kontekste yra ribotas. Dalis modelių orientuojasi į atskiras saugumo dimensijas – technologinę apsaugą, atitiktį reikalavimams ar rizikų valdymą – ir nepakankamai susieja strateginį, taktinį, operacinį ir technologinį valdymo lygmenis į vientisą valdymo sistemą. Tarpinstitucinių kibernetinio saugumo valdymo modelių analizė papildomai išryškino koordinavimo, atsakomybių paskirstymo, informacijos mainų ir bendro incidentų valdymo svarbą, kuri ypač aktuali tarpusavyje susijusių e. sveikatos organizacijų ir informacinių sistemų aplinkoje.

Remiantis atlikta modelių analize, suformuluoti kibernetinio saugumo valdymo modelio kūrimo principai ir reikalavimai. Funkcinių ir nefunkcinių reikalavimų

išskyrimas leido apibrėžti pagrindines valdymo funkcijas bei modelio savybes, reikalingas jo pritaikymui skirtingose e. sveikatos organizacijose. Ypatingas dėmesys skirtas modelio sistemiškumui, pritaikomumui, lankstumui, valdymo lygmenų sąveikai, brandos vertinimui ir galimybei atsižvelgti į skirtingą organizacijų pasirengimo lygį bei kintančią reguliacinę aplinką.

Toliau pagrįstos kibernetinio saugumo valdymo modelio kūrimo prielaidos. Šiame kontekste išskirti strateginis, taktinis, operacinis ir technologinis valdymo lygmenys, pabrėžiant jų tarpusavio sąveiką ir skirtingas valdymo funkcijas. Toks struktūravimas leidžia kibernetinį saugumą e. sveikatos sistemoje vertinti ne kaip atskirą technologinę funkciją, bet kaip integruotą vadybinį procesą, kuriame strateginiai sprendimai siejami su taktiniu planavimu, operaciniu įgyvendinimu ir technologinėmis kontrolės priemonėmis.

Informacijos srautų saugumo analizė parodė, kad duomenų judėjimas tarp institucijų, informacinių sistemų, procesų ir naudotojų sudaro reikšmingą kibernetinio saugumo valdymo aspektą. Todėl saugumo sprendimai turi būti orientuoti ne tik į pavienių informacinių sistemų ar technologinių komponentų apsaugą, bet ir į jų tarpusavio sąveikos bei informacijos mainų valdymą visos e. sveikatos ekosistemos mastu. Atsakomybių paskirstymo analizė savo ruožtu išryškino aiškiai apibrėžtų vaidmenų, atskaitomybės ir koordinavimo mechanizmų reikšmę mažinant valdymo fragmentiškumą ir užtikrinant nuoseklesnį kibernetinio saugumo reikalavimų įgyvendinimą.

Šių prielaidų pagrindu suformuotas kibernetinio saugumo valdymo modelis e. sveikatos sistemai. Antrojoje disertacijos dalyje jis pateikiamas kaip teorinis ir konceptualus pagrindas, struktūruojantis pagrindinius kibernetinio saugumo valdymo elementus. Modelis apima strateginį, taktinį, operacinį ir technologinį valdymo lygmenis, funkcines saugumo dimensijas, informacijos srautus, grįžtamojo ryšio mechanizmus ir e. sveikatos sistemos kontekstą. Modelio struktūra sudaro pagrindą tolesniam ekspertiniam vertinimui ir jo tikslinimui remiantis empirinio tyrimo rezultatais.

Antrojoje disertacijos dalyje taip pat pagrindžiama empirinio tyrimo metodologija. Tyrimo tikslas, uždaviniai ir tiriamieji klausimai susiejami su teorinėje analizėje identifikuotomis kibernetinio saugumo valdymo problemomis ir suformuoto modelio vertinimo poreikiu. Tyrimo dizainas pasirinktas atsižvelgiant į tyrimo objekto – e. sveikatos sistemos kibernetinio saugumo valdymo – kompleksiškumą ir poreikį gauti gilumines ekspertines įžvalgas apie valdymo organizavimą, praktines valdymo spragas, skirtingų valdymo lygmenų sąveiką, modelio taikymo galimybes ir jo tobulinimo kryptis.

Ekspertinis tyrimas pasirinktas kaip pagrindinė empirinio tyrimo strategija, leidžianti analizuoti ne tik formaliai apibrėžtus kibernetinio saugumo valdymo sprendimus, bet ir ekspertų profesine patirtimi grindžiamus vertinimus apie jų praktinį įgyvendinimą. Antrojoje dalyje apibrėžta tyrimo imtis, ekspertų atrankos kriterijai, duomenų rinkimo priemonės ir duomenų analizės metodai. Tokia metodologinė struktūra užtikrina nuoseklų ryšį tarp teorinio modelio, tiriamųjų klausimų ir empirinio jo vertinimo.

Atsižvelgiant į tyrimo pobūdį, atsakymai į tiriamuosius klausimus grindžiami

temine ekspertinių interviu analize, kategorijų ir subkategorijų išskyrimu, pasikartojančių ekspertinių įžvalgų vertinimu ir papildomu ekspertų ranginių vertinimų suderinamumo įvertinimu taikant Kendall konkordacijos koeficientą W.

Apibendrinant galima teigti, kad antrojoje disertacijos dalyje suformuotas teoriškai ir metodologiškai pagrįstas pagrindas kibernetinio saugumo valdymo modeliui ir jo ekspertiniam vertinimui. Joje apibrėžtos modelio kūrimo prielaidos, valdymo lygmenų ir funkcinių dimensijų sąveika, modelio struktūrinė logika, tyrimo dizainas, ekspertų atrankos kriterijai bei duomenų analizės procedūros. Tai sudaro pagrindą trečiojoje disertacijos dalyje analizuoti ekspertų identifikuojamas valdymo problemas, įvertinti modelio struktūrą ir, remiantis tyrimo rezultatais, jį patikslinti.

TREČIOSIOS DALIES APŽVALGA: EMPIRINIO TYRIMO REZULTATAI IR KIBERNETINIO SAUGUMO VALDYMO MODELIO E. SVEIKATOS SISTEMOS TOBULINIMUI TIKSLINIMAS

Trečiojoje disertacijos dalyje pateikiama empirinio tyrimo rezultatų analizė ir jų integravimas į kibernetinio saugumo valdymo modelio tikslinimą e. sveikatos sistemos kontekste. Šioje dalyje antrojoje disertacijos dalyje suformuotas kibernetinio saugumo valdymo modelis vertinamas remiantis ekspertinių interviu duomenimis, siekiant nustatyti jo struktūrinių elementų atitiktį praktikoje identifikuojamoms valdymo problemoms, išryškinti tobulintinas sritis ir pagrįsti tolesnį modelio tikslinimą.

Pirmiausia pristatoma ekspertinio tyrimo analizės struktūra ir tyrime dalyvavusių ekspertų profesinis profilis. Ekspertų įžvalgos leidžia įvertinti kibernetinio saugumo valdymo organizavimą sveikatos sektoriaus organizacijose, identifikuoti pagrindines valdymo spragas ir atskleisti rizikų bei incidentų valdymo praktikos ypatumus. Tyrimo rezultatai parodė, kad e. sveikatos kibernetinio saugumo problemos nėra siejamos vien su technologinių priemonių trūkumais. Ekspertų vertinimuose jos atsiskleidžia kaip platesnės vadybinės ir organizacinės problemos, susijusios su atsakomybių paskirstymu, valdymo lygmenų tarpusavio sąveika, rizikų valdymo nuoseklumu, darbuotojų kompetencijomis, vadovybės įsitraukimu ir tarpinstituciniu koordinavimu.

Toliau atliekama teminė ekspertinių interviu analizė, kuria siekiama išskirti pasikartojančias temas, problemines sritis ir jų tarpusavio sąsajas. Analizėje daugiausia dėmesio skiriama strateginio, taktinio, operacinio ir technologinio valdymo sąveikai, organizacinės atsakomybės klausimams, rizikų ir incidentų valdymui, procesų brandai bei teisinio reglamentavimo ir praktinio įgyvendinimo sąsajoms. Ši analizė sudaro pagrindą atsakyti į TK1–TK4 tiriamuosius klausimus. Atsakymai formuojami remiantis ekspertų pasisakymų turiniu, kategorijų ir subkategorijų išskyrimu, pasikartojančių įžvalgų vertinimu bei jų tarpusavio sąsajomis. Papildomai ekspertų ranginių vertinimų suderinamumui įvertinti taikomas Kendall konkordacijos koeficientas W.

TK1 analizė atskleidė, kad ekspertų vertinimu kibernetinio saugumo valdymui e. sveikatos organizacijose būdingi fragmentiškumo požymiai, pasireiškiantys techninio požiūrio dominavimu, nepakankamai aiškiu atsakomybių paskirstymu,

nenuosekliu rizikų valdymu ir ribotu strateginio lygmens įsitraukimu. TK2 rezultatai parodė, kad strateginio, taktinio, operacinio ir technologinio kibernetinio saugumo valdymo lygmenų integracija e. sveikatos organizacijose išlieka nepakankamai nuosekli. TK3 analizė atskleidė, kad ekspertai kibernetinio saugumo valdymo struktūrizuotumą sieja su veiksmingesniu incidentų valdymu, ypač pabrėždami aiškiai apibrėžtas atsakomybes, formalizuotą eskalavimo tvarką, nuoseklius informacijos srautus ir organizacinį mokymąsi po incidentų. TK4 rezultatai parodė, kad siūlomo kibernetinio saugumo valdymo modelio galimą indėlį ekspertai sieja su aiškesniu atsakomybių paskirstymu, nuoseklesniu rizikų valdymu, geresniu pasirengimu kibernetiniams incidentams ir sistemingesniu kibernetinio saugumo brandos vertinimu.

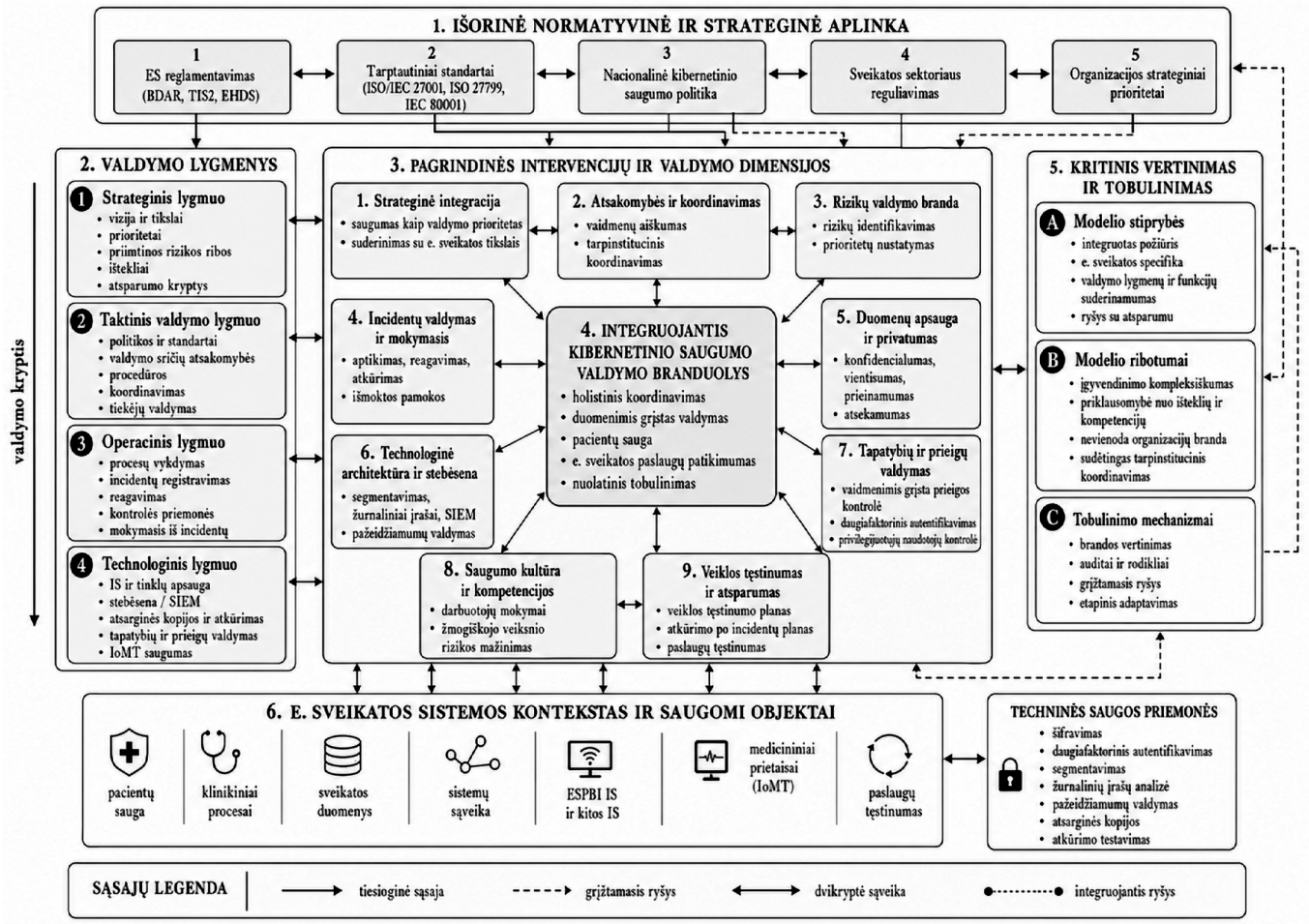
Remiantis ekspertinio tyrimo rezultatais, trečiojoje dalyje pereinama prie kibernetinio saugumo valdymo modelio tikslinimo. Ekspertų įžvalgos leido nustatyti svarbiausias kibernetinio saugumo valdymo sritis ir pagrįsti, kurie modelio elementai turi būti sustiprinti. Modelio tikslinimas orientuojamas į strateginio valdymo stiprinimą, aiškesnį taktinį koordinavimą, operacinių procesų nuoseklumą, technologinių priemonių susiejimą su organizaciniais sprendimais, rizikų ir incidentų valdymo ciklišKumą, atsakomybių paskirstymą, grįžtamojo ryšio mechanizmus, brandos vertinimą ir nuolatinį tobulinimą. Papildomai išryškinami rizikomis grindžiamo išteklių planavimo ir tarpinstitucinio koordinavimo mechanizmai, leidžiantys modelį glaudžiau susieti su praktiniais e. sveikatos organizacijų valdymo procesais.

Atskirai analizuojamas patikslinto kibernetinio saugumo valdymo modelio ekspertinis vertinimas. Vertinamas modelio tinkamumas, struktūrinis nuoseklumas, praktinio taikymo galimybės, stiprybės, ribotumai ir tobulinimo kryptys. Ekspertų vertinimai parodė, kad modelio struktūra gali būti taikoma kaip pagrindas kibernetinio saugumo valdymo spragoms identifikuoti, atsakomybių paskirstymui struktūruoti, rizikų ir incidentų valdymui struktūruoti bei prioritetinėms tobulinimo kryptims nustatyti. Modelio praktinis taikymas siejamas su organizacijos brandos lygiu, vadovybės įsitraukimu, darbuotojų kompetencijomis, turimais ištekliais ir tarpinstitucinio koordinavimo kokybe.

Siekiant modelį pritaikyti ne tik kaip konceptualią valdymo struktūrą, bet ir kaip praktinį vertinimo instrumentą, trečiojoje dalyje parengta e. sveikatos kibernetinio saugumo valdymo brandos vertinimo metodika. Ji grindžiama modelyje išskirtais valdymo lygmenimis ir funkcinėmis dimensijomis bei leidžia sistemiškai vertinti atskirų valdymo sričių brandą. Vertinimui taikoma 0–4 balų brandos skalė, o bendram organizacijos kibernetinio saugumo valdymo brandos lygiui nustatyti apskaičiuojamas apibendrintas brandos indeksas. Praktiniam metodikos taikymui parengta vertinimo matrica, susiejanti vertinimo kriterijus, galimus įrodymus ir brandos lygius. Tokia metodika sudaro galimybę identifikuoti silpniausias valdymo sritis, nustatyti prioritetines tobulinimo kryptis ir periodiškai vertinti kibernetinio saugumo valdymo pažangą.

Apibendrinant galima teigti, kad trečiojoje disertacijos dalyje ekspertinio tyrimo rezultatai sudaro empirinį pagrindą patikslinti kibernetinio saugumo valdymo modelį e. sveikatos sistemos kontekste ir išryškinti svarbiausius jo vadybinius mechanizmus. Tyrimo rezultatai parodė, kad e. sveikatos kibernetinio saugumo valdymas turi būti

grindžiamas ne pavienėmis technologinėmis priemonėmis, bet integruotu vadybiniu požiūriu, apimančiu strateginių, taktinių, operacinių ir technologinių sprendimų sąveiką, atsakomybių paskirstymą, rizikomis grindžiamą sprendimų priėmimą, rizikų ir incidentų valdymą, tarpinstitucinį koordinavimą, brandos vertinimą ir organizacinį mokymąsi. Šios dalies rezultatai sudaro pagrindą galutinėms disertacijos išvadoms ir praktinėms rekomendacijoms dėl modelio taikymo e. sveikatos sistemos kibernetinio saugumo valdymo tobulinimui.



2 pav. Patikslintas kibernetinio saugumo valdymo modelis e. sveikatos sistemos tobulinimui.

Šaltinis: sudaryta autorės

IŠVADOS

1. Teorinė analizė parodė, kad e. sveikatos kibernetinio saugumo valdymas yra kompleksinis socio-techninis ir vadybinis reiškinys, kurio veiksmingumą lemia ne pavienės kontrolės priemonės, o strateginių, organizacinių, procesinių ir technologinių sprendimų tarpusavio sąveika. Todėl kibernetinis saugumas turi būti integruojamas į bendrą organizacijos valdymo sistemą, siejant jį su atsakomybių paskirstymu, rizikų valdymu, veiklos tęstinumu ir nuolatiniu brandos didinimu.
   1.1. E. sveikatos sistemos kibernetinio saugumo valdymo kompleksiškumą lemia informacinių sistemų tarpusavio priklausomybė, jautrių sveikatos duomenų srautai ir skirtingų organizacijų atsakomybės ribos. Teorinė analizė parodė, kad vien techninėmis kontrolės priemonėmis ar formalia atitiktimi grindžiamas požiūris nėra pakankamas, nes kibernetinio saugumo rezultatus lemia ir rizikų valdymo, atsakomybių paskirstymo, incidentų valdymo, veiklos tęstinumo bei nuolatinio tobulinimo procesų tarpusavio sąveika.
   1.2. Teorinė analizė parodė, kad tarptautiniai standartai, informacijos saugumo valdymo sistemos, rizikų valdymo metodikos ir brandos modeliai sudaro reikšmingą metodinį pagrindą, tačiau jų taikymas e. sveikatos sistemoje reikalauja papildomo vadybinio pritaikymo. Šiame kontekste esminę reikšmę įgyja ne tik technologinių ir duomenų apsaugos reikalavimų įgyvendinimas, bet ir jų susiejimas su tarpinstituciniu koordinavimu, atsakomybių paskirstymu, veiklos tęstinumo valdymu ir nuosekliu kibernetinio atsparumo stiprinimu.
   1.3. Teorinė analizė pagrindė integruoto kibernetinio saugumo valdymo poreikį, kai strateginiai, organizaciniai, procesiniai ir technologiniai sprendimai siejami tarpusavyje, o ne įgyvendinami kaip atskiros saugumo priemonės. Vadybiniu požiūriu esminę reikšmę įgyja aiškus atsakomybių paskirstymas, rizikomis grindžiamas sprendimų priėmimas, skirtingų valdymo lygmenų koordinavimas ir nuolatinis procesų vertinimas bei tobulinimas.
2. Sisteminė e. sveikatos sistemų kibernetinių incidentų ir atakų analizė parodė, kad kibernetinio atsparumo pažeidžiamumą lemia kompleksinė technologinių, organizacinių, procesinių ir žmogiškųjų veiksnių sąveika. Todėl incidentų valdymo veiksmingumas priklauso ne tik nuo techninių apsaugos priemonių, bet ir nuo organizacijos gebėjimo integruoti rizikų vertinimą, reagavimą, veiklos atkūrimą ir organizacinį mokymąsi į nuoseklų valdymo procesą.
   2.1. Sisteminė incidentų ir atakų analizė atskleidė, kad jų poveikio mastą e. sveikatos sistemoje lemia ne vien techninis pažeidimo pobūdis, bet ir kritinių paslaugų priklausomybė nuo informacinių sistemų, tarpsisteminių sąsajų sudėtingumas, trečiųjų šalių dalyvavimas bei organizacijų pasirengimas valdyti sutrikimus. Didžiausia rizika kyla tais atvejais, kai duomenų

konfidencialumo, vientisumo ar prieinamumo pažeidimai kartu paveikia paslaugų tęstinumą, todėl incidentų valdymas turi būti siejamas su veiklos kritiškumo vertinimu ir organizacinio atsparumo užtikrinimu.

2.2. Sisteminė incidentų ir atakų analizė parodė, kad e. sveikatos sistemos kibernetinis atsparumas priklauso nuo organizacijos gebėjimo nuosekliai vykdyti visą incidentų valdymo ciklą – nuo grėsmių identifikavimo ir reagavimo iki veiklos atkūrimo bei poįvykiminės analizės. Tyrimo rezultatai išryškino, kad būtent incidentų valdymo tęstinumas ir grįžtamojo ryšio integravimas į vadybinius sprendimus yra reikšmingi veiksniai, siejant operacinį reagavimą su ilgalaikiu organizaciniu pasirengimu.

2.3. Sisteminė incidentų ir atakų analizė atskleidė, kad e. sveikatos kibernetinis atsparumas priklauso nuo tarpusavyje susietų vadybinių ir organizacinių mechanizmų – rizikų valdymo, prieigos kontrolės, duomenų apsaugos, tiekėjų priežiūros, darbuotojų kompetencijų stiprinimo ir organizacinio mokymosi po incidentų. Šių mechanizmų integravimas į bendrą valdymo sistemą sudaro pagrindą nuosekliau valdyti ne tik pavienes grėsmes, bet ir jų galimą sisteminį poveikį e. sveikatos paslaugų tęstinumui.

3. Teorinės analizės ir e. sveikatos sistemos valdymo ypatumų pagrindu suformuotas koncepcinis kibernetinio saugumo valdymo modelis, integruojantis strateginį, taktinį, operacinį ir technologinį valdymo lygmenis. Modelio struktūra sudaro pagrindą nuosekliai susieti atsakomybių paskirstymą, rizikų ir incidentų valdymą, informacijos srautų kontrolę bei kibernetinio saugumo brandos vertinimą.

3.1. Koncepcinio modelio struktūroje išskirti strateginis, taktinis, operacinis ir technologinis valdymo lygmenys sudaro sąlygas kibernetinio saugumo sprendimus vertinti kaip tarpusavyje susijusią vadybinių veiksmų sistemą. Toks struktūravimas leidžia aiškiau atskirti sprendimų priėmimo, jų įgyvendinimo ir kontrolės atsakomybes bei susieti jas su skirtingais e. sveikatos sistemos valdymo lygmenimis.

3.2. Koncepcinio modelio struktūra pagrįsta tarpusavyje susietomis vadybinėmis ir funkcinėmis dimensijomis – atsakomybių paskirstymu, rizikų ir incidentų valdymu, informacijos srautų kontrole, duomenų apsauga, teisine atitiktimi, brandos vertinimu ir nuolatiniu tobulinimu. Šių dimensijų integravimas į strateginį, taktinį, operacinį ir technologinį valdymo lygmenis sudaro pagrindą nuosekliai koordinuoti sprendimų priėmimą, atsakomybę ir kontrolės priemonių įgyvendinimą visame e. sveikatos sistemos valdymo cikle.

3.3. Parengtas koncepcinis modelis suformavo analitinį pagrindą empiriškai vertinti e. sveikatos kibernetinio saugumo valdymo spragas ir nustatyti, kurie vadybiniai mechanizmai turi būti stiprinami praktiniame modelio taikyme. Ekspertinio tyrimo rezultatai leido patikslinti modelio struktūrą, išryškinant atsakomybių paskirstymo, valdymo lygmenų koordinavimo,

rizikomis grindžiamo sprendimų priėmimo ir organizacinio mokymosi reikšmę.

4. Ekspertinio tyrimo rezultatai atskleidė, kad e. sveikatos organizacijų kibernetinio saugumo valdymo ribotumai pirmiausia siejami su valdymo fragmentacija, nepakankamai aiškiu atsakomybių paskirstymu ir silpna skirtingų valdymo lygmenų sąveika. Šių problemų sprendimui būtinas nuoseklesnis rizikų ir incidentų valdymo integravimas į organizacijos sprendimų priėmimo procesus, aiškesnis koordinavimas ir sisteminis organizacinis mokymasis.
    4.1. Ekspertinių interviu rezultatai parodė, kad e. sveikatos organizacijose kibernetinio saugumo valdymo trūkumai pirmiausia siejami su nepakankamu jo integravimu į bendrą organizacijos valdymą. Ekspertų vertinimu, neaiškiai paskirstytos atsakomybės, ribotas vadovybės įsitraukimas ir nepakankamas tarpinstitucinis koordinavimas silpnina galimybes nuosekliai įgyvendinti kibernetinio saugumo reikalavimus praktikoje.
    4.2. TK1–TK4 analizė parodė, kad pagrindinės e. sveikatos kibernetinio saugumo valdymo problemos kyla ne dėl pavienių techninių trūkumų, bet dėl nepakankamo valdymo procesų tarpusavio susiejimo. Ekspertų vertinimu, didžiausią reikšmę turi aiškus atsakomybių paskirstymas, strateginio, taktinio, operacinio ir technologinio valdymo lygmenų koordinavimas bei nuoseklus rizikų ir incidentų valdymas. Šie rezultatai sudarė empirinį pagrindą modelį tikslinti stiprinant jo vadybinius mechanizmus.
    4.3. Atsižvelgiant į ekspertų identifikuotas problemas ir empirinio tyrimo rezultatus, koncepcinis modelis buvo patikslintas, daugiau dėmesio skiriant vadybiniams jo įgyvendinimo mechanizmams. Modelyje sustiprinti atsakomybių paskirstymo, padalinių ir institucijų koordinavimo, rizikomis grindžiamo išteklių planavimo, incidentų valdymo, grįžtamojo ryšio ir brandos vertinimo elementai. Šie papildymai leidžia modelį glaudžiau susieti su praktiniais e. sveikatos organizacijų valdymo procesais ir ekspertų nustatytomis problemomis.
5. Ekspertinis patikslinto kibernetinio saugumo valdymo modelio vertinimas parodė, kad jo struktūra yra logiškai nuosekli, atitinka ekspertų identifikuotus e. sveikatos kibernetinio saugumo valdymo poreikius ir gali būti taikoma kaip praktinis pagrindas valdymo spragoms nustatyti bei tobulinimo prioritetams formuoti.
    5.1. Ekspertinių interviu rezultatai sudarė pagrindą įvertinti siūlomo modelio praktinę reikšmę e. sveikatos organizacijų kibernetinio saugumo valdymui. Ekspertai modelio taikymo galimybes siejo su aiškesniu atsakomybių paskirstymu, rizikomis grindžiamu išteklių planavimu, nuoseklesniu rizikų ir incidentų valdymu, tarpinstitucinio koordinavimo stiprinimu bei kryptingesniu kibernetinio saugumo brandos didinimu.
    5.2. Ekspertų vertinimu, didžiausią praktinę reikšmę turi modelyje numatytas aiškesnis atsakomybių paskirstymas, incidentų valdymo struktūrizavimas ir valdymo sprendimų pritaikymas e. sveikatos sistemos specifikai.

Šie elementai sudaro vadybinį pagrindą nuosekliau organizuoti kibernetinio saugumo procesus ir mažinti ekspertų identifikuotą atotrūkį tarp formalių reikalavimų ir jų praktinio įgyvendinimo.

5.3. Kendall konkordacijos koeficientas parodė aukštą ekspertų vertinimų suderinamumą, todėl gauti rezultatai laikytini nuosekliais tyrimo imties ribose. Ekspertinis vertinimas pagrindė patikslinto modelio tinkamumą valdymo fragmentiškumui identifikuoti, atsakomybių aiškumui stiprinti ir rizikų bei incidentų valdymo sąsajoms struktūruoti.

6. Teorinės ir empirinės analizės rezultatai leido suformuluoti patikslinto kibernetinio saugumo valdymo modelio taikymo rekomendacijas, orientuotas į vadybinių sprendimų nuoseklumą, atsakomybių paskirstymą, rizikomis grindžiamą išteklių planavimą, tarpinstitucinį koordinavimą ir periodinį kibernetinio saugumo brandos vertinimą. Šių mechanizmų integravimas sudaro praktinį pagrindą sistemiškai taikyti modelį e. sveikatos organizacijų valdymo procesuose.

6.1. Patikslinto modelio taikymas grindžiamas jo integravimu į pagrindinius organizacijos valdymo procesus – strateginį planavimą, atsakomybių paskirstymą, rizikų ir incidentų valdymą, išteklių planavimą bei veiklos rezultatų stebėseną. Toks taikymo principas leidžia modelį naudoti ne tik kibernetinio saugumo būklei aprašyti, bet ir kaip vadybinį instrumentą valdymo spragoms nustatyti, prioritetams pagrįsti ir organizacijos brandos pokyčiams vertinti.

6.2. Parengtos rekomendacijos operacionalizuoja patikslinto modelio taikymą, susiedamos jo struktūrinius elementus su konkrečiais vadybiniais veiksmais: valdymo būklės vertinimu, prioritetų nustatymu, atsakomybių paskirstymu, rizikų ir incidentų valdymo integravimu bei technologinių sprendimų derinimu su organizacijos valdymo tikslais. Toks taikymo principas sudaro prielaidas nuosekliau vertinti kibernetinio saugumo brandą ir kryptingai planuoti jos tobulinimą.

6.3. Praktinio taikymo gairės papildo patikslintą modelį konkrečiais jo įgyvendinimo mechanizmais ir sudaro sąlygas modelį taikyti kaip nuoseklaus kibernetinio saugumo valdymo tobulinimo pagrindą. Modelio taikymo rezultatai turėtų būti vertinami periodiškai, analizuojant brandos pokyčius, incidentų valdymo rodiklius, veiklos tęstinumo būklę ir kitus organizacijos parengtį atspindinčius kriterijus. Toks vertinimas leistų pagrįstai nustatyti, kokiu mastu modelio taikymas siejasi su kibernetinio saugumo valdymo pažanga konkrečios e. sveikatos organizacijos kontekste.

REKOMENDACIJOS

• *Patikslintą kibernetinio saugumo valdymo modelį e. sveikatos sistemos tobulinimui taikyti kaip strateginį e. sveikatos sistemos kibernetinio saugumo valdymo pagrindą.*

Rekomenduojama patikslintą modelį naudoti kaip orientacinę valdymo struktūrą, padedančią e. sveikatos sistemos kibernetinį saugumą susieti su strateginiais sveikatos sektoriaus skaitmenizavimo, paslaugų tęstinumo, pacientų saugos ir kritinės infrastruktūros apsaugos tikslais. Modelis turėtų būti integruojamas į nacionalinio ir organizacinio lygmens strateginius dokumentus, kibernetinio saugumo politikas, informacijos saugumo valdymo sistemas ir e. sveikatos plėtros programas.

Taikant modelį, kibernetinis saugumas neturėtų būti suprantamas kaip atskira techninė funkcija. Jis turėtų būti vertinamas kaip integruota valdymo sritis, kurioje strateginiai sprendimai, organizacinės atsakomybės, rizikų valdymas, incidentų valdymas, technologinės priemonės ir teisinė atitiktis veikia kaip tarpusavyje susiję elementai.

• *Modelį naudoti kaip diagnostinę priemonę kibernetinio saugumo valdymo spragoms nustatyti.*

Rekomenduojama patikslintą modelį taikyti atliekant e. sveikatos organizacijų kibernetinio saugumo valdymo būklės vertinimą. Vertinimas turėtų apimti modelyje išskirtus valdymo lygmenis – strateginį, taktinį, operacinį ir technologinį – bei funkcines dimensijas: rizikų valdymą, incidentų valdymą, atsakomybių paskirstymą, informacijos srautų saugumą, duomenų apsaugą, teisinę atitiktį, brandos vertinimą ir nuolatinį tobulinimą.

Praktikoje tai galėtų būti įgyvendinama kaip periodinis savęs vertinimas arba vidaus audito priemonė. Kiekviena organizacija, taikydama modelį, turėtų įvertinti, kurie modelio elementai jau yra įgyvendinti, kurie veikia fragmentiškai, o kurių trūksta. Tokiu būdu modelis leistų ne tik aprašyti esamą situaciją, bet ir nustatyti prioritetines tobulinimo kryptis, susijusias su atsakomybių aiškumu, rizikų valdymo integracija, incidentų valdymo pasirengimu, technologinių priemonių pakankamumu ir organizaciniu mokymusi.

• *Modelio pagrindu aiškiai paskirstyti atsakomybes tarp strateginio, taktinio, operacinio ir technologinio valdymo lygmenų.*

Empirinio tyrimo rezultatai parodė, kad viena iš svarbiausių e. sveikatos kibernetinio saugumo valdymo problemų yra atsakomybių neapibrėžtumas ir valdymo fragmentiškumas. Todėl rekomenduojama modelį naudoti kaip atsakomybių paskirstymo pagrindą. Strateginiame lygmenyje turėtų būti apibrėžta vadovybės atsakomybė už kibernetinio saugumo prioritetus, rizikos toleranciją, išteklių skyrimą ir saugumo rodiklių vertinimą. Taktiniame lygmenyje turėtų būti nustatytos koordinavimo funkcijos, politikų ir procedūrų rengimas, padalinių bendradarbiavimo mechanizmai. Operaciniame lygmenyje turėtų būti apibrėžti kasdieniai saugumo procesai, incidentų registravimas, reagavimas, eskalavimas ir atkūrimas. Technologiniame lygmenyje turėtų

būti numatytos konkrečios kontrolės priemonės, susijusios su prieigos valdymu, stebėsena, infrastruktūros apsauga ir duomenų saugumu. Tokiu būdu modelis galėtų būti taikomas kaip praktinė priemonė atsakomybių matricai sudaryti.

• *Kibernetinio saugumo išteklių paskirstymą grįsti rizikų vertinimu ir nustatytais valdymo prioritetais.*

Rekomenduojama sprendimus dėl finansinių, žmogiškųjų ir technologinių išteklių skyrimo kibernetiniam saugumui tiesiogiai sieti su organizacijos rizikų vertinimo rezultatais, kritinių e. sveikatos paslaugų reikšmingumu ir nustatytomis valdymo spragomis. Tokiu būdu išteklių paskirstymas būtų grindžiamas ne pavieniais technologiniais poreikiais ar reaktyviu reagavimu į incidentus, bet nuosekliu organizacijos kibernetinio saugumo prioritetų vertinimu.

Taikant patikslintą modelį, aukščiausio lygmens vadovybė turėtų periodiškai vertinti, ar turimi ištekliai atitinka nustatytą rizikos lygį ir pasirinktus kibernetinio saugumo tikslus. Tai sudarytų prielaidas kryptingiau planuoti investicijas, darbuotojų kompetencijų stiprinimą, technologinių priemonių diegimą ir veiklos tęstinumui reikalingus sprendimus.

• *Stiprinti tarpinstitucinį kibernetinio saugumo valdymo koordinavimą e. sveikatos sistemoje.*

E. sveikatos sistemos kibernetinis saugumas priklauso nuo skirtingų institucijų, sveikatos priežiūros įstaigų, informacinių sistemų valdytojų ir technologinių paslaugų teikėjų tarpusavio sąveikos. Todėl rekomenduojama aiškiai apibrėžti tarpinstitucinio koordinavimo tvarką, atsakomybes, informacijos apsikeitimo principus ir veiksmus kibernetinių incidentų metu.

Praktikoje tai gali būti įgyvendinama nustatant nuolatinius koordinavimo mechanizmus, bendrus kontaktinius taškus, suderintas incidentų eskalavimo procedūras ir periodines bendras pratybas. Tokia sąveika sudarytų prielaidas greičiau keistis informacija apie rizikas ir incidentus, sumažintų atsakomybių dubliavimąsi ir padėtų nuosekliau įgyvendinti kibernetinio saugumo reikalavimus visoje e. sveikatos sistemoje.

• *Modelio pagrindu integruoti rizikų ir incidentų valdymą į vieną nuoseklų ciklą.*

Rekomenduojama modelį taikyti siekiant susieti rizikų valdymą, incidentų valdymą ir organizacinį mokymąsi. Rizikų vertinimas neturėtų apsiriboti formaliu rizikų dokumentavimu. Jis turėtų būti naudojamas priimant sprendimus dėl saugumo priemonių prioritetų, finansavimo, infrastruktūros atnaujinimo, prieigos kontrolės, darbuotojų mokymų ir incidentų valdymo pasirengimo.

Incidentų valdymo srityje modelis turėtų būti taikomas kaip procesinė schema, apimanti incidentų identifikavimą, registravimą, klasifikavimą, eskalavimą, reagavimą, komunikaciją, paslaugų atkūrimą ir analizę po incidento. Po kiekvieno reikšmingo incidento turėtų būti vertinama, kokie modelio elementai veikė tinkamai, o kurie reikalauja tobulinimo.

• *Patikslintą modelį taikyti technologinių saugumo priemonių planavimui ir prioritetų nustatymui.*

Rekomenduojama modelį naudoti ne tik vadybiniams, bet ir technologiniams sprendimams planuoti. Modelis turėtų padėti susieti technologines saugumo priemones su rizikų vertinimu, organizacijos brandos lygiu ir e. sveikatos sistemos veiklos kritiškumu. Planuojant technologines priemones, ypatingas dėmesys turėtų būti skiriamas tapatybės ir prieigos valdymui, naudotojų teisių kontrolei, privilegijuotų naudotojų priežiūrai, saugumo įvykių stebėsenai, žurnalinių įrašų analizei, duomenų apsaugai, atsarginių kopijų valdymui, medicininių įrenginių saugumui ir tarpsisteminių integracijų apsaugai.

Modelis taip pat turėtų būti naudojamas vertinant, ar technologiniai sprendimai nėra diegiami fragmentiškai. Technologinės investicijos turėtų būti pagrįstos ne vien techniniu poreikiu, bet ir jų poveikiu visai kibernetinio saugumo valdymo sistemai. Tai leistų užtikrinti, kad technologinis lygmuo būtų susietas su strateginiais ir taktiniais sprendimais, o saugumo priemonės būtų planuojamos ne pavieniui, bet kaip vientisos saugumo architektūros dalis.

• *Modelį integruoti į e. sveikatos sistemos tobulinimo ir projektų valdymo procesus.*

Kadangi modelis orientuotas į e. sveikatos sistemos projektavimo, diegimo, administravimo ir tobulinimo etapus, rekomenduojama jį taikyti ne tik eksploatuojamų sistemų saugumo vertinimui, bet ir naujų e. sveikatos sprendimų planavimui. Kiekviename e. sveikatos sistemos plėtros ar modernizavimo projekte modelio elementai turėtų būti naudojami kaip kontroliniai klausimai: ar nustatytos atsakomybės, ar atliktas rizikų vertinimas, ar numatyti incidentų valdymo veiksmai, ar užtikrintas informacijos srautų saugumas, ar numatytas sistemos stebėsenos ir tobulinimo mechanizmas.

Toks modelio taikymas leistų kibernetinį saugumą integruoti ne po sistemos įdiegimo, bet nuo ankstyvųjų projektavimo ir diegimo etapų. Tai ypač svarbu e. sveikatos sistemoje, kur nauji sprendimai dažnai susiję su jautrių sveikatos duomenų tvarkymu, skirtingų informacinių sistemų sąveika ir paslaugų prieinamumo reikalavimais.

MOKSLINIŲ PUBLIKACIJŲ SĄRAŠAS

1. Limba, T.; Lelešienė, L.; Novogreckas, S. (2022). Using WEB 2.0 and Social Networking in Education: Theoretical Insights. *EDULEARN22: 14th International Conference on Education and New Learning Technologies,* Palma, Spain, 4th–6th of July, 2022. doi: 10.21125/edulearn.2022.0834
2. Limba, T.; Lelešienė, L.; Novogreckas, S. (2022). Social and Digital Media in Education. *EDULEARN22: 14th International Conference on Education and New Learning Technologies,* Palma, Spain, 4th–6th of July, 2022. doi: 10.21125/edulearn.2022.1468
3. Tvaronavičienė, M.; Plėta, T.; Beretas, C. P.; Lelešienė, L. (2022). Analysis of the Critical Infrastructure Cyber Security Policy. *Insights into Regional Development,* 4(1), 26–39. https://doi.org/10.9770/ird.2022.4.1(2)
4. Katina, J.; Plėta, T.; Petkevičius, R.; Lelešienė, L. (2023). Industrial Control Systems (ICS) Cyber Prediction Model. *Insights into Regional Development,* 5(1), 86–96. https://doi.org/10.9770/ird.2023.5.1(6)
5. Limba, T.; Lelešienė, L.; Novogreckas, S.; Kowalewska, A. (2023). Knowledge and Innovation Management. *EDULEARN23: 15th International Conference on Education and New Learning Technologies,* Palma, Spain, 3rd–5th of July, 2023. doi: 10.21125/edulearn.2023.0826
6. Limba, T.; Lelešienė, L.; Novogreckas, S.; Kowalewska, A. (2024). Exploring the Impact of Artificial Intelligence on Educational Paradigms: Unleashing the Potential. *EDULEARN24: 16th International Conference on Education and New Learning Technologies,* Palma, Spain, 1st–3rd of July, 2024. doi: 10.21125/edulearn.2024.1087
7. Limba, T.; Lelešienė, L.; Novogreckas, S.; Kowalewska, A. (2024). Harnessing Artificial Intelligence, Chatbots and Robots for Transformative Education: Exploring the Convergence. *EDULEARN24: 16th International Conference on Education and New Learning Technologies,* Palma, Spain, 1st–3rd of July, 2024. doi: 10.21125/edulearn.2024.1094
8. Limba, T.; Lelešienė, L.; Lelešius, V.; Novogreckas, S. (2025). Lessons from Large-Scale International Projects: Insights for Global Education, Collaboration, and AI Integration. *INTED2025 Proceedings: 19th International Technology, Education and Development Conference,* Valencia, Spain, 3rd–5th of March, 2025. doi: 10.21125/inted.2025.1639
9. Limba, T.; Lelešienė, L.; Lelešius, V.; Novogreckas, S. (2025). Education in the Age of AI: Exploring the Role of ChatGPT, Innovations, and Future Directions. *INTED2025 Proceedings: 19th International Technology, Education and Development Conference,* Valencia, Spain, 3rd–5th of March, 2025. doi: 10.21125/inted.2025.1638
10. Limba, T.; Lelešienė, L.; Lelešius, V. (2026). Cybersecurity Competence Gaps in E-Health Systems: Educational Needs Identified Through Expert Evaluation. *ICERI2026: 19th International Conference of Education, Research and Innovation,*

Seville, Spain, 9th–11th of November, 2026. [Accepted for publication]

11. Limba, T.; Lelešienė, L.; Lelešius, V. (2026). Comparing Cybersecurity Approaches in European E-Health Systems: Lessons from Estonia, Finland and Denmark for Professional Education. *ICERI2026: 19th International Conference of Education, Research and Innovation*, Seville, Spain, 9th–11th of November, 2026. [Accepted for publication]

PRANEŠIMAI MOKSLINĖSE KONFERENCIJOSE

1. Limba, T.; Lelešienė, L.; Novogreckas, S. Using WEB 2.0 and Social Networking in Education: Theoretical Insights. *EDULEARN22: 14th International Conference on Education and New Learning Technologies,* Palma, Spain, 4th–6th of July, 2022.
2. Limba, T.; Lelešienė, L.; Novogreckas, S. Social and Digital Media in Education. *EDULEARN22: 14th International Conference on Education and New Learning Technologies,* Palma, Spain, 4th–6th of July, 2022.
3. Limba, T.; Lelešienė, L.; Novogreckas, S.; Kowalewska, A. Knowledge and Innovation Management. *EDULEARN23: 15th International Conference on Education and New Learning Technologies,* Palma, Spain, 3rd–5th of July, 2023.
4. Limba, T.; Lelešienė, L.; Novogreckas, S.; Kowalewska, A. Exploring the Impact of Artificial Intelligence on Educational Paradigms: Unleashing the Potential. *EDULEARN24: 16th International Conference on Education and New Learning Technologies,* Palma, Spain, 1st–3rd of July, 2024.
5. Limba, T.; Lelešienė, L.; Novogreckas, S.; Kowalewska, A. Harnessing Artificial Intelligence, Chatbots and Robots for Transformative Education: Exploring the Convergence. *EDULEARN24: 16th International Conference on Education and New Learning Technologies,* Palma, Spain, 1st–3rd of July, 2024.
6. Limba, T.; Lelešienė, L.; Lelešius, V.; Novogreckas, S. Lessons from Large-Scale International Projects: Insights for Global Education, Collaboration, and AI Integration. *INTED2025: 19th International Technology, Education and Development Conference,* Valencia, Spain, 3rd–5th of March, 2025.
7. Limba, T.; Lelešienė, L.; Lelešius, V.; Novogreckas, S. Education in the Age of AI: Exploring the Role of ChatGPT, Innovations, and Future Directions. *INTED2025: 19th International Technology, Education and Development Conference,* Valencia, Spain, 3rd–5th of March, 2025.
8. Limba, T.; Lelešienė, L.; Lelešius, V. Cybersecurity Competence Gaps in E-Health Systems: Educational Needs Identified Through Expert Evaluation. *ICERI2026: 19th International Conference of Education, Research and Innovation,* Seville, Spain, 9th–11th of November, 2026.
9. Limba, T.; Lelešienė, L.; Lelešius, V. Comparing Cybersecurity Approaches in European E-Health Systems: Lessons from Estonia, Finland and Denmark for Professional Education. *ICERI2026: 19th International Conference of Education, Research and Innovation,* Seville, Spain, 9th–11th of November, 2026.

GYVENIMO APRAŠYMAS

Išsilavinimas

2020 – 2026	Vadybos mokslo krypties Mykolo Romerio universiteto doktorantė
2018 – 2020	Kibernetinio saugumo valdymo magistras, Mykolo Romerio universitetas

Darbo patirtis

Nuo 2023 m.	Valstybinės duomenų apsaugos inspekcijos Informacinių technologijų skyriaus vedėja
Nuo 2022 m.	Mykolo Romerio universiteto lektorė
Nuo 2024 m.	Vilniaus universiteto verslo mokyklos dėstytoja praktikė
2020 – 2023 m.	Nacionalinis kibernetinio saugumo centras, specialistė

MYKOLAS ROMERIS UNIVERSITY

Lina Lelešienė

EVALUATION OF CYBERSECURITY MANAGEMENT MODEL FOR DEVELOPING E-HEALTH SYSTEM

Summary of Doctoral Dissertation
Social Sciences, Management (S 003)

Vilnius, 2026

This doctoral dissertation has been prepared during the period of 2020–2026 at Mykolas Romeris University under the doctoral program right conferred to Vytautas Magnus University, Klaipėda University, Mykolas Romeris University and Vilnius University by the order of the Minister of Education, Science and Sport of the Republic of Lithuania No. V-160 dated February 22, 2019.

Scientific Supervisor:

Prof. Dr. Tadas Limba (Mykolas Romeris University, Social Sciences, Management, S 003).

The doctoral dissertation will be defended in the board of management research of Vytautas Magnus University, Klaipėda University, Mykolas Romeris University and Vilnius University Šiauliai Academy:

Chairperson:

Prof. Dr. Andrius Stasiukynas (Mykolas Romeris University, Social Sciences, Management, S 003).

Members:

Prof. Dr. Vida Davidavičienė (Vilnius Gediminas Technical University, Social Sciences, Management, S 003);

Prof. Dr. Iveta Reinholde (University of Latvia, Republic of Latvia, Social Sciences, Political Science, S 002);

Prof. Dr. Rimantas Stašys (Klaipėda University, Social Sciences, Management, S 003);

Prof. Dr. Jolita Vveinhardt (Vytautas Magnus University, Social Sciences, Management, S 003).

The doctoral dissertation will be defended at the open meeting of the Scientific Council in the field of Management on 10 November 2026, at 10:00 a.m. at Mykolas Romeris University, I-414 auditorium.

Address: Ateities St. 20, LT-08303 Vilnius, Lithuania.

SUMMARY

The development of e-health systems is fundamentally transforming the organisation of healthcare services and the management of health data. An increasing number of healthcare processes are taking place in the digital environment, ranging from electronic health records and e-prescriptions to patient registration, the exchange of medical documentation, and data transmission between healthcare institutions. Such solutions facilitate faster information exchange, more efficient organisation of services, and greater convenience for both patients and healthcare professionals.

At the same time, increasing digitalisation creates new cybersecurity challenges. E-health systems process highly sensitive personal health data, while the interconnection of different information systems means that a security breach in one part of the system may affect other participants within the ecosystem. Data breaches, unauthorised access, and disruptions to e-prescription services, patient portals, or medical document exchange may have consequences not only for data protection, but also for service continuity and patient trust. Therefore, cybersecurity in e-health should be understood not merely as the application of technical safeguards, but as a coherent management process encompassing risk assessment, allocation of responsibilities, incident management, data protection, and continuous system improvement.

In recent years, the healthcare sector has increasingly been identified as one of the most vulnerable targets of cyberattacks because it combines the protection of sensitive data, continuity of critical services, and often limited organisational resources. This demonstrates that security management based solely on isolated technical measures is insufficient. Healthcare institutions are particularly attractive targets because of the highly sensitive data they manage, the critical nature of their infrastructure, and the frequently limited resources available for implementing advanced security measures. Ransomware attacks, personal data breaches, service disruptions, unauthorised access to e-health information systems, and compromises of network-connected medical devices pose risks not only to personal data protection, but also to the continuity of healthcare services and may consequently have a direct impact on patient safety.

For this reason, cybersecurity management in this dissertation is examined not as a collection of isolated technical measures, but as a coherent management process adapted to the structure and operational characteristics of the e-health system. At the regulatory level, the importance of cybersecurity continues to increase, while regulatory frameworks, international standards, and related requirements, including the NIS2 Directive, the GDPR, ISO/IEC 27001, ISO/IEC 27005:2018, ISO/IEC 27035-1:2023, ISO/IEC 27701:2019, and ISO/IEC 27032:2023, establish more stringent requirements for information security and risk management, emphasising the need for systematic information security management, the integration of risk assessment processes, and the continuous enhancement of organisational security maturity. Nevertheless, healthcare organisations often encounter difficulties in translating these standards and requirements into practical management decisions. Consequently, this dissertation substantiates the need for a cybersecurity management model that integrates the

provisions of international standards, national regulation, and the organisational and technological specificities of the e-health system.

The relevance of the topic is further reinforced by organisational factors. The ability of healthcare institutions to manage cybersecurity depends not only on technology, but also on employee competencies, the allocation of responsibilities, internal procedures, and management involvement. Empirical studies demonstrate that cybersecurity culture, employees' knowledge and skills, clearly defined management processes, and the effectiveness of organisational structures influence how effectively healthcare institutions are able to implement security measures and respond to emerging threats. However, there remains a lack of empirical models enabling the assessment and comparison of cybersecurity management maturity across different levels of the e-health system. Therefore, the scientific contribution associated with the development and evaluation of a cybersecurity management model may also have considerable practical value by improving decision-making, supporting more rational resource allocation, and strengthening organisational resilience to cyber threats.

In this dissertation, cybersecurity management in the e-health system is treated as both a scientific and a practical problem arising from the complexity of e-health infrastructure, increasing cyber risks, and the need to align management decisions with the specific structure of the e-health system.

Although information security management has been widely examined in the fields of economics and management, existing knowledge remains insufficient for the development of cybersecurity management models specifically adapted to e-health systems. Researchers emphasise that the protection of critical infrastructure requires a comprehensive approach, while the e-health system represents one of the most important innovations in the healthcare sector and is characterised by highly sensitive data and complex processes. Although its economic, social, and organisational benefits are evident, the development of methods capable of assessing the value created by such systems remains challenging. Various evaluation models applied in practice assist in measuring efficiency and optimising processes; however, their application differs depending on system objectives, stakeholders, and contextual conditions. Because e-health services are directly related to human health and are particularly sensitive from the users' perspective, a cybersecurity management model specifically adapted to this field is required. Despite the relevance of the subject, cybersecurity management in the context of e-health remains insufficiently explored internationally.

The dissertation seeks to develop a cybersecurity management model that could be effectively applied in the development and administration of the e-health system. One of the most significant challenges facing e-health infrastructure is the insufficient security of information systems. This dissertation assumes that the cybersecurity management model developed in the study may create conditions for more coherent and efficient development of e-health solutions. Contemporary technological development is resulting in an increasingly intensive transfer of sensitive data into the digital environment, making cybersecurity an increasingly relevant issue for both organisations and individual users. As dependence on digital services grows, so does vulnerability,

which in turn increases the interest of researchers and society in cybersecurity issues. Effective management of emerging risks requires the systematic identification of potential threats, assessment of their possible impact, and development of preventive measures enabling timely risk mitigation.

A synthesis of the scientific literature analysed in the dissertation reveals several problematic aspects associated with the development of a cybersecurity management model in the context of e-health system development. First, difficulties arise in selecting and adapting the most appropriate cybersecurity models that could be applied to the development and improvement of e-health infrastructure. The need to clearly define the intended outcomes is also emphasised, as these determine the selection of an appropriate management model and the logic of its application. Finally, the literature highlights the need to develop evaluation criteria that enable analysis not only of individual system components, but also of the entire e-health ecosystem as an integrated entity, thereby providing a basis for combining different indicators within a coherent and systematic assessment framework.

Thus, in this dissertation, cybersecurity management modelling is analysed as an approach for systematically integrating the development of e-health infrastructure, risk management, incident management, data protection, and the conditions required for strengthening cyber resilience.

Scientific problem – what should a cybersecurity management model be in order to ensure effective improvement of the e-health system and reduce risks associated with cyber threats and information system vulnerabilities?

Research object – the evaluation of a cybersecurity management model in the context of the e-health system.

Research aim – to develop a cybersecurity management model for the improvement of the e-health system, thereby creating conditions for strengthening the resilience of the e-health system to cyber threats.

Research Objectives

1. To analyse the theoretical aspects, principles, and existing models of cybersecurity management, as well as the specific characteristics of cybersecurity management in the context of e-health information system integration, data protection, and cyber resilience.
2. To conduct a systematic analysis of cyber incidents and cyberattacks affecting e-health systems.
3. To develop a conceptual cybersecurity management model oriented towards the design, implementation, administration, and improvement stages of the e-health system.
4. To refine the developed cybersecurity management model for the improvement of the e-health system on the basis of the problems identified by experts and the results obtained from the empirical research.
5. To evaluate, from an expert perspective, the suitability and practical applicability of the developed cybersecurity management model for the improvement of

the e-health system, its correspondence with the practices of healthcare organisations, and its potential limitations in application.

6. To develop recommendations for the application of the refined cybersecurity management model and its integration into e-health system improvement processes.

Research Methods

The dissertation applies comparative analysis of scientific literature, international standards, and legislation in order to identify the directions, relationships, and differences in the application of cybersecurity management principles, models, and methodologies in the context of the e-health system. The systematisation and synthesis of theoretical sources make it possible to identify the principal factors contributing to cyber incidents and vulnerabilities of e-health infrastructure, as well as to develop an initial conceptual cybersecurity management model oriented towards the design, implementation, administration, and improvement processes of the e-health system. European Commission artificial intelligence language tools were used for the translation of certain scientific sources and quotations.

The empirical part of the research employs a qualitative research method – semi-structured expert interviews involving professionals working in the fields of cybersecurity management, e-health system administration, strategic planning, and the implementation of technological solutions. Expert insights are used to refine the elements of the initial model, assess their practical relevance, identify systemic gaps, and formulate improvements to the model that reflect the actual management conditions of the e-health system.

Document analysis is additionally applied to compare and assess expert insights in relation to regulatory requirements, guidelines, strategic documents, and, where relevant, internal organisational documents. Interview data are analysed using thematic analysis, systematically identifying recurring themes, problematic areas, and their relationships with the structural levels and functional dimensions of the model. Based on the results of the theoretical analysis and empirical research, the cybersecurity management model is refined and improved, and the dissertation concludes by formulating generalised scientific and practical conclusions and recommendations regarding the application of the model in e-health system improvement processes.

Statements to Be Defended

1. The effectiveness of e-health cybersecurity management depends on its integration into overall organisational management, management involvement, and a clear allocation of responsibilities.
2. Fragmentation in cybersecurity management is reduced through coherent interaction between the strategic, tactical, operational, and technological management levels.
3. The refined cybersecurity management model provides a methodological basis for identifying management gaps and substantiating priority areas for improvement.

Scientific Novelty and Practical Significance of the Dissertation

Cybersecurity management in the context of the e-health system is an interdisciplinary field encompassing issues related to information technology, management, law, public administration, and health sciences. Although a considerable body of research worldwide addresses cybersecurity issues, many studies analyse the phenomenon within the boundaries of a single scientific discipline without sufficiently considering the broader context of organisational, process-related, and regulatory factors. Consequently, cybersecurity is often approached in a fragmented manner – either as a technological challenge or as an issue of legal and regulatory compliance – even though effective cybersecurity requires an integrated approach based on knowledge from multiple scientific disciplines.

The scientific novelty of this dissertation lies in its comprehensive examination of cybersecurity management through the integration of technological, organisational, process-related, and legal aspects of the e-health system. Based on the analysis of scientific literature, international standards, and practical cases involving e-health systems, the dissertation identifies cybersecurity management vulnerabilities, risk factors, and weaknesses in e-health infrastructure interaction that have significant implications for system reliability. The research also analyses international practices related to cybersecurity incidents in e-health systems, thereby enabling the identification of trends emerging in international research and practice and the identification of particularly vulnerable system components. In contrast to existing cybersecurity models, the model proposed in this dissertation integrates strategic, organisational, process-related, and technological management levels specifically within the context of the e-health ecosystem and is empirically substantiated through expert research conducted in the national context.

The practical significance of the dissertation is reflected in several aspects. First, the cybersecurity management model developed in the dissertation can be applied to the improvement, design, and administration processes of the e-health system, thereby creating conditions for reducing infrastructure vulnerability and strengthening the system's resilience to cyber threats. Second, the model's evaluation criteria and structural elements can be used by healthcare managers and policymakers when making decisions concerning the enhancement of cybersecurity management maturity, resource allocation, and the planning of risk mitigation measures. Third, the research results provide a methodological basis for e-health policy development, the adaptation of standards, and the integration of cybersecurity management principles into strategic management documents.

The model proposed in the dissertation can be applied not only during the development and operation of the e-health system, but also when conducting periodic security assessments of the e-health system, planning infrastructure modernisation, and strengthening organisational preparedness to respond to cyber threats. In this way, the research contributes to the sustainable development of the e-health system and creates conditions for the development of safer and more reliable e-health services capable of strengthening public trust in Lithuania.

Structure of the Dissertation

The dissertation consists of three logically interconnected parts.

The first part of the dissertation examines the theoretical aspects of cybersecurity management. It analyses the development of the cybersecurity concept, its principal principles and objectives, and contemporary cyber threats and risks, with particular emphasis on those relevant to the e-health sector. It also examines information security management systems, international standards, including ISO/IEC 27001 and ISO/IEC 27005, the requirements of the NIS2 Directive, and cybersecurity maturity models. The first part establishes the theoretical basis for the subsequent development and empirical evaluation of the model.

The second part of the dissertation presents the conceptual framework for developing the structure of a cybersecurity management model for the improvement of the e-health system and provides the methodological foundation for the research. This part analyses existing theoretical and practical cybersecurity management models, formulates the principles and requirements for model development, and defines the assumptions underlying the model structure, management levels, information flows, and allocation of responsibilities. It also provides a detailed substantiation of the research methodology, describing the research design, expert selection, data collection instruments, and data analysis methods applied.

The third part of the dissertation presents and analyses the empirical research results. Based on expert interview data, the level of cybersecurity management in healthcare institutions is assessed, key cybersecurity management gaps are identified, risk and incident management practices are analysed, and a thematic analysis of expert insights is conducted. The empirical results are used to identify critical areas of cybersecurity management and to refine the proposed management model. An expert evaluation of the proposed cybersecurity management model is also conducted. The suitability of the model and its potential application within the e-health system are analysed, its strengths and limitations are assessed, substantiated directions for improvement are formulated, and its practical applicability across different organisational and institutional contexts is discussed.

The dissertation concludes with generalised conclusions and recommendations that systematically summarise the main research findings, assess the achievement of the research aim, and formulate practical and scientific recommendations for improving cybersecurity management in the e-health system (see Figure 1).

.

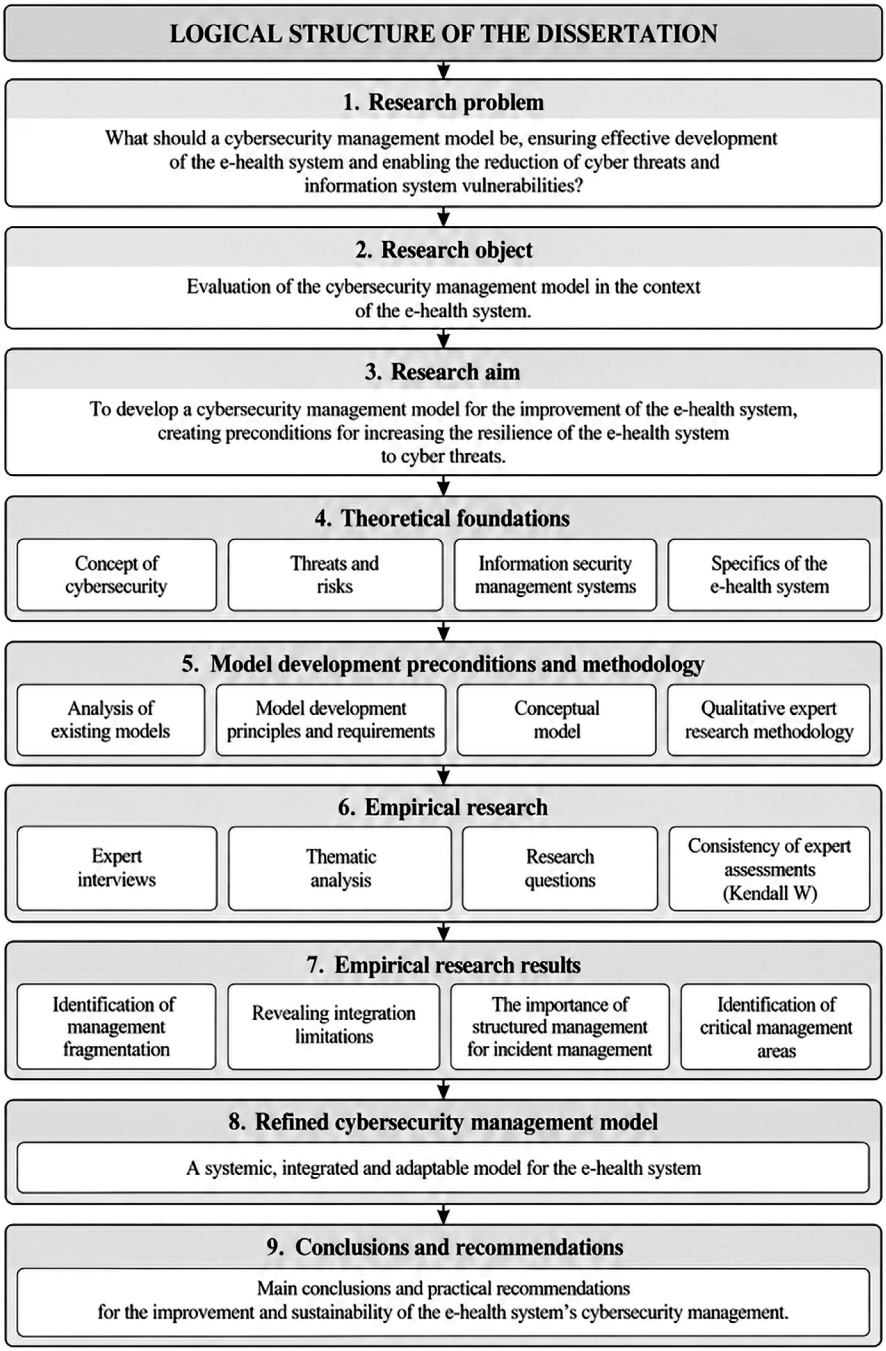


Figure 1. Logical Structure of the Dissertation.

Source: compiled by the author

REVIEW OF PART ONE: THEORETICAL ASPECTS OF CYBERSECURITY GOVERNANCE

The first part of the dissertation establishes the theoretical and conceptual foundation required to substantiate the cybersecurity management model in the context of the e-health system and to conduct the subsequent empirical research. This part analyses the concept of cybersecurity, its significance in a digitalised environment, and the specific challenges arising in critical sectors, with particular attention to the healthcare system.

The analysis of the development of the cybersecurity concept demonstrated that, in the contemporary context, cybersecurity can no longer be understood merely as a set of technical protection measures. In the scientific literature and international regulatory documents, it is increasingly associated with organisations' ability to manage risks, ensure business continuity, and adapt to a changing threat environment. Such an approach encompasses technological, organisational, legal, and human factors and supports the position adopted in this dissertation that cybersecurity should be integrated into the overall organisational management system rather than remain solely the responsibility of information technology units.

The analysis of cyber threats, risks, and incidents revealed that contemporary threats are characterised by dynamism and complexity, while their impact is determined not only by technical vulnerabilities but also by organisational, process-related, and human weaknesses. The analysis of approaches to cybersecurity incident classification showed that purely technical classification models are insufficient for assessing the impact of incidents on complex socio-technical systems. In the e-health sector, multidimensional classifications encompassing technological, organisational, clinical, and business continuity aspects are particularly significant, as cyber incidents may affect not only information security but also service availability, patient safety, and the reliability of health data.

The analysis of risk factors in the e-health sector showed that cyber risks emerge from the interaction of technological, organisational, regulatory, and human factors. The integration of information systems, the connection of medical devices to networks, the high sensitivity of health data, business continuity requirements, and fragmented governance structures create an environment in which general-purpose risk management models are insufficient. This substantiates the need to develop a cybersecurity management model adapted to the structure of the e-health system, its operational logic, interinstitutional relationships, and organisational responsibilities.

The first part also analyses information security management systems, international standards, including ISO/IEC 27001 and ISO/IEC 27005, as well as the European Union cybersecurity regulatory framework, including the NIS2 Directive. The analysis demonstrated that standards and regulatory requirements provide a significant methodological basis for cybersecurity, but are not sufficient on their own to ensure coherent security management. In practice, their implementation is constrained by formalisation, fragmented governance, and the insufficient integration of security

requirements into organisational decision-making processes. Therefore, regulatory compliance is treated in this dissertation not as an independent administrative function, but as one of the dimensions of an integrated cybersecurity management system.

The analysis of cybersecurity management in the healthcare sector revealed the high structural and functional complexity of the e-health system. The interaction of information systems, intensive data exchange, the involvement of different institutions, the integration of medical devices, and high service availability requirements create a need for a systemic approach to cybersecurity management. From a management perspective, this requires the integration of strategic planning, clear allocation of responsibilities, risk and incident management, interinstitutional coordination, technological control measures, data protection, business continuity, and maturity assessment.

In summary, the first part of the dissertation establishes the theoretical basis for moving from general cybersecurity concepts towards the development of a management model specifically adapted to the e-health system. The identified patterns relating to threats, risks, incidents, and governance gaps substantiate the need to treat cybersecurity in the e-health system as an integrated management process. These insights provide the logical foundation for the second part of the dissertation, which analyses cybersecurity management models, formulates the assumptions underlying model development, and substantiates the empirical research methodology.

REVIEW OF PART TWO: DEVELOPMENT OF THE STRUCTURE OF A CYBERSECURITY GOVERNANCE MODEL FOR IMPROVING THE E-HEALTH SYSTEM AND RESEARCH METHODOLOGY

The second part of the dissertation moves from the theoretical analysis of cybersecurity concepts and related challenges to the development of a cybersecurity management model for the e-health system and the methodological substantiation of the empirical research. This part serves as a bridge between the theoretical insights developed in the first part and the assumptions underlying model development, its structural logic, and empirical evaluation.

First, a systematic analysis of cybersecurity management models was conducted, covering both theoretical approaches and models applied in practice across different sectors, including healthcare and critical infrastructure. The analysis showed that existing models provide a significant methodological basis for structuring cybersecurity processes, managing risks, and assessing organisational maturity; however, their direct application in the context of the e-health system is limited. Some models focus on separate security dimensions, such as technological protection, regulatory compliance, or risk management, and do not sufficiently integrate the strategic, tactical, operational, and technological management levels into a coherent governance system. The analysis of interinstitutional cybersecurity management models further highlighted

the importance of coordination, allocation of responsibilities, information exchange, and joint incident management, which are particularly relevant in an environment of interconnected e-health organisations and information systems.

Based on the analysis of existing models, the principles and requirements for the development of the cybersecurity management model were formulated. The distinction between functional and non-functional requirements made it possible to define the key management functions and model characteristics necessary for its application across different e-health organisations. Particular attention was paid to the systemic nature of the model, its applicability, flexibility, interaction between management levels, maturity assessment, and its ability to accommodate different levels of organisational preparedness and a changing regulatory environment.

The assumptions underlying the development of the cybersecurity management model were then substantiated. In this context, the strategic, tactical, operational, and technological management levels were distinguished, with emphasis placed on their interaction and distinct management functions. Such structuring makes it possible to view cybersecurity in the e-health system not as a separate technological function, but as an integrated management process in which strategic decisions are linked to tactical planning, operational implementation, and technological control measures.

The analysis of information flow security demonstrated that the movement of data between institutions, information systems, processes, and users constitutes a significant aspect of cybersecurity management. Therefore, security measures should be directed not only at protecting individual information systems or technological components, but also at managing their interconnections and information exchange across the entire e-health ecosystem. The analysis of the allocation of responsibilities further highlighted the importance of clearly defined roles, accountability, and coordination mechanisms in reducing governance fragmentation and ensuring more consistent implementation of cybersecurity requirements.

On the basis of these assumptions, a cybersecurity management model for the e-health system was developed. In the second part of the dissertation, it is presented as a theoretical and conceptual framework that structures the main elements of cybersecurity management. The model encompasses the strategic, tactical, operational, and technological management levels, functional security dimensions, information flows, feedback mechanisms, and the specific context of the e-health system. The structure of the model provides the basis for subsequent expert evaluation and refinement on the basis of empirical research results.

The second part of the dissertation also substantiates the methodology of the empirical research. The research aim, objectives, and research questions are linked to the cybersecurity management problems identified in the theoretical analysis and to the need to evaluate the developed model. The research design was selected by taking into account the complexity of the research object – cybersecurity management in the e-health system – and the need to obtain in-depth expert insights into governance arrangements, practical management gaps, interaction between different management levels, possibilities for applying the model, and directions for its improvement.

Expert research was selected as the principal empirical research strategy, as it enables the analysis not only of formally defined cybersecurity management solutions, but also of expert assessments based on professional experience regarding their practical implementation. The second part defines the research sample, expert selection criteria, data collection instruments, and data analysis methods. This methodological structure ensures a consistent relationship between the theoretical model, the research questions, and its empirical evaluation.

Given the nature of the research, the answers to the research questions are based on thematic analysis of expert interviews, the identification of categories and subcategories, the assessment of recurring expert insights, and an additional evaluation of the agreement among expert rankings using Kendall's coefficient of concordance W.

In summary, the second part of the dissertation establishes a theoretically and methodologically grounded basis for the cybersecurity management model and its expert evaluation. It defines the assumptions underlying model development, the interaction between management levels and functional dimensions, the structural logic of the model, the research design, expert selection criteria, and data analysis procedures. This provides the basis for the third part of the dissertation, in which the management problems identified by experts are analysed, the structure of the model is evaluated, and the model is refined on the basis of the research results.

REVIEW OF PART THREE: EMPIRICAL RESEARCH RESULTS AND REFINEMENT OF THE CYBERSECURITY GOVERNANCE MODEL FOR IMPROVING THE E-HEALTH SYSTEM

The third part of the dissertation presents an analysis of the empirical research results and their integration into the refinement of the cybersecurity management model in the context of the e-health system. In this part, the cybersecurity management model developed in the second part of the dissertation is evaluated on the basis of expert interview data in order to determine the extent to which its structural elements correspond to the management problems identified in practice, to highlight areas requiring improvement, and to substantiate the further refinement of the model.

First, the structure of the expert study analysis and the professional profiles of the participating experts are presented. Expert insights make it possible to assess the organisation of cybersecurity management in healthcare sector organisations, identify key management gaps, and reveal the specific characteristics of risk and incident management practices. The research results showed that cybersecurity problems in e-health are not associated solely with deficiencies in technological measures. In the experts' assessments, these problems emerge as broader managerial and organisational issues related to the allocation of responsibilities, interaction between management levels, consistency of risk management, employee competencies, management

involvement, and interinstitutional coordination.

Thematic analysis of the expert interviews is then conducted in order to identify recurring themes, problematic areas, and the relationships between them. The analysis focuses primarily on the interaction between strategic, tactical, operational, and technological management, issues of organisational responsibility, risk and incident management, process maturity, and the relationship between legal regulation and practical implementation. This analysis provides the basis for answering Research Questions RQ1–RQ4. The answers are formulated on the basis of the content of the experts' statements, the identification of categories and subcategories, the assessment of recurring insights, and the relationships between them. In addition, Kendall's coefficient of concordance W is applied to assess the level of agreement among the experts' ranked evaluations.

The analysis of RQ1 revealed that, according to the experts, cybersecurity management in e-health organisations exhibits signs of fragmentation, reflected in the dominance of a technical perspective, insufficiently clear allocation of responsibilities, inconsistent risk management, and limited involvement at the strategic level. The results of RQ2 showed that the integration of strategic, tactical, operational, and technological cybersecurity management levels in e-health organisations remains insufficiently coherent. The analysis of RQ3 revealed that experts associate a more structured approach to cybersecurity management with more effective incident management, particularly emphasising clearly defined responsibilities, formalised escalation procedures, coherent information flows, and organisational learning following incidents. The results of RQ4 showed that experts associate the potential contribution of the proposed cybersecurity management model with clearer allocation of responsibilities, more consistent risk management, improved preparedness for cyber incidents, and more systematic assessment of cybersecurity maturity.

Based on the results of the expert study, the third part proceeds to the refinement of the cybersecurity management model. Expert insights made it possible to identify the most significant areas of cybersecurity management and to substantiate which elements of the model require strengthening. The refinement of the model focuses on strengthening strategic management, ensuring clearer tactical coordination, improving the consistency of operational processes, linking technological measures with organisational decisions, establishing cyclical risk and incident management processes, clarifying the allocation of responsibilities, strengthening feedback mechanisms, assessing maturity, and supporting continuous improvement. Additional emphasis is placed on risk-based resource planning and interinstitutional coordination mechanisms, enabling the model to be more closely aligned with practical management processes in e-health organisations.

The expert evaluation of the refined cybersecurity management model is analysed separately. The assessment addresses the suitability and structural coherence of the model, possibilities for its practical application, its strengths and limitations, and potential directions for further improvement. The expert evaluations showed that the structure of the model can be applied as a basis for identifying gaps in cybersecurity

management, structuring the allocation of responsibilities, improving the consistency of risk and incident management, and determining priority areas for improvement. The practical application of the model is associated with the organisation's level of maturity, management involvement, employee competencies, available resources, and the quality of interinstitutional coordination.

In order to enable the model to be applied not only as a conceptual management framework but also as a practical assessment instrument, a methodology for assessing cybersecurity management maturity in e-health was developed in the third part of the dissertation. The methodology is based on the management levels and functional dimensions distinguished within the model and enables the systematic assessment of maturity across individual areas of management. A 0–4 maturity scale is applied, while an aggregated maturity index is calculated to determine the overall level of cybersecurity management maturity within an organisation. For the practical application of the methodology, an assessment matrix was developed linking assessment criteria, possible evidence, and maturity levels. This methodology makes it possible to identify the weakest areas of management, determine priority directions for improvement, and periodically assess progress in cybersecurity management.

In summary, the results of the expert study presented in the third part of the dissertation provide an empirical basis for refining the cybersecurity management model in the context of the e-health system and for highlighting its key managerial mechanisms. The research results showed that cybersecurity management in e-health should be based not on isolated technological measures, but on an integrated managerial approach encompassing the interaction of strategic, tactical, operational, and technological decisions, allocation of responsibilities, risk-based decision-making, risk and incident management, interinstitutional coordination, maturity assessment, and organisational learning. The results of this part provide the basis for the final conclusions of the dissertation and for practical recommendations concerning the application of the model to the improvement of cybersecurity management in the e-health system.

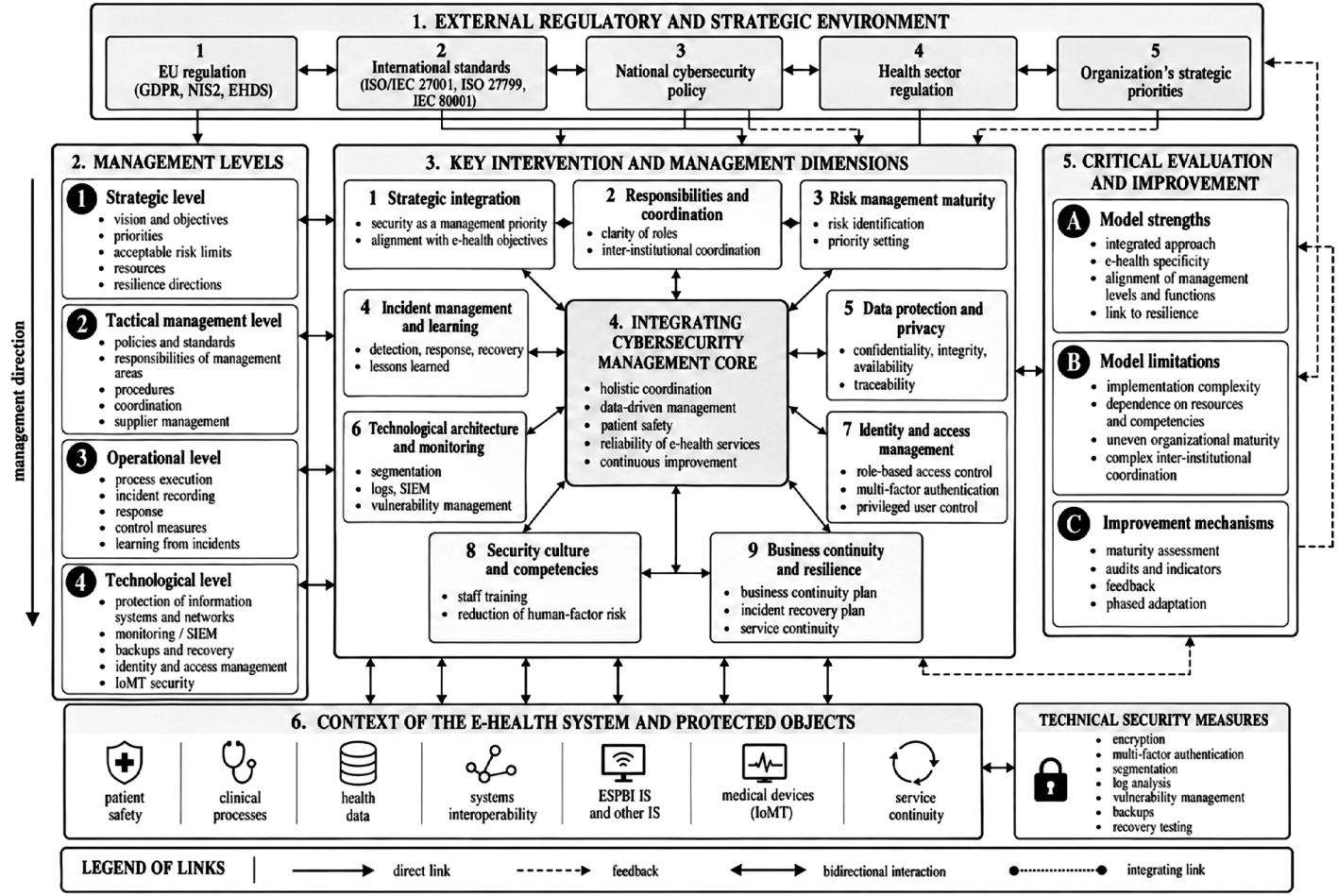


Figure 2. Refined Cybersecurity Management Model for E-Health System Improvement

Source: compiled by the author

CONCLUSIONS

1. The theoretical analysis demonstrated that cybersecurity management in e-health is a complex socio-technical and managerial phenomenon whose effectiveness is determined not by individual control measures, but by the interaction of strategic, organisational, process-related, and technological decisions. Cybersecurity should therefore be integrated into the overall organisational management system by linking it to the allocation of responsibilities, risk management, business continuity, and continuous maturity improvement.
    1.1. The complexity of cybersecurity management in the e-health system is determined by the interdependence of information systems, flows of sensitive health data, and the boundaries of responsibility among different organisations. The theoretical analysis demonstrated that an approach based solely on technical controls or formal compliance is insufficient, as cybersecurity outcomes are also influenced by the interaction between risk management, allocation of responsibilities, incident management, business continuity, and continuous improvement processes.
    1.2. The theoretical analysis showed that international standards, information security management systems, risk management methodologies, and maturity models provide a significant methodological foundation; however, their application in the e-health system requires additional managerial adaptation. In this context, particular importance is attached not only to the implementation of technological and data protection requirements, but also to linking them with interinstitutional coordination, the allocation of responsibilities, business continuity management, and the consistent strengthening of cyber resilience.
    1.3. The theoretical analysis substantiated the need for integrated cybersecurity management in which strategic, organisational, process-related, and technological decisions are interconnected rather than implemented as separate security measures. From a management perspective, particular importance is attached to a clear allocation of responsibilities, risk-based decision-making, coordination across different management levels, and continuous process assessment and improvement.
2. The systematic analysis of cyber incidents and attacks affecting e-health systems demonstrated that vulnerability in terms of cyber resilience is determined by the complex interaction of technological, organisational, process-related, and human factors. Therefore, the effectiveness of incident management depends not only on technical safeguards, but also on an organisation's ability to integrate risk assessment, response, business recovery, and organisational learning into a coherent management process.
    2.1. The systematic analysis of incidents and attacks revealed that the scale of their impact within the e-health system is determined not only by the technical nature of a breach, but also by the dependence of critical

services on information systems, the complexity of inter-system connections, third-party involvement, and organisations' preparedness to manage disruptions. The greatest risk arises when breaches of data confidentiality, integrity, or availability simultaneously affect service continuity; therefore, incident management should be linked to assessments of operational criticality and the assurance of organisational resilience.

2.2. The systematic analysis of incidents and attacks showed that the cyber resilience of the e-health system depends on an organisation's ability to consistently implement the entire incident management cycle, from threat identification and response to business recovery and post-incident analysis. The research results highlighted that continuity in incident management and the integration of feedback into managerial decision-making are significant factors linking operational response with long-term organisational preparedness.

2.3. The systematic analysis of incidents and attacks revealed that e-health cyber resilience depends on interconnected managerial and organisational mechanisms, including risk management, access control, data protection, supplier oversight, the enhancement of employee competencies, and organisational learning following incidents. Integrating these mechanisms into the overall management system provides a basis for more consistent management not only of individual threats, but also of their potential systemic impact on the continuity of e-health services.

3. On the basis of the theoretical analysis and the specific characteristics of e-health system management, a conceptual cybersecurity management model was developed that integrates the strategic, tactical, operational, and technological management levels. The structure of the model provides a basis for coherently linking the allocation of responsibilities, risk and incident management, information flow control, and cybersecurity maturity assessment.

3.1. The strategic, tactical, operational, and technological management levels distinguished within the conceptual model make it possible to view cybersecurity decisions as an interconnected system of managerial actions. Such structuring enables a clearer distinction between responsibilities for decision-making, implementation, and control and allows them to be linked to the different management levels of the e-health system.

3.2. The structure of the conceptual model is based on interconnected managerial and functional dimensions, including the allocation of responsibilities, risk and incident management, information flow control, data protection, legal compliance, maturity assessment, and continuous improvement. Integrating these dimensions across the strategic, tactical, operational, and technological management levels provides a basis for the consistent coordination of decision-making, responsibility, and

implementation of control measures throughout the e-health system management cycle.

3.3. The developed conceptual model provided an analytical basis for the empirical assessment of cybersecurity management gaps in e-health and for identifying which managerial mechanisms should be strengthened in the practical application of the model. The results of the expert study enabled the structure of the model to be refined by highlighting the importance of the allocation of responsibilities, coordination between management levels, risk-based decision-making, and organisational learning.

4. The results of the expert study revealed that the limitations of cybersecurity management in e-health organisations are primarily associated with governance fragmentation, insufficiently clear allocation of responsibilities, and weak interaction between different management levels. Addressing these problems requires more consistent integration of risk and incident management into organisational decision-making processes, clearer coordination, and systematic organisational learning.

4.1. The results of the expert interviews showed that deficiencies in cybersecurity management within e-health organisations are primarily associated with its insufficient integration into overall organisational management. According to the experts, unclear allocation of responsibilities, limited management involvement, and insufficient interinstitutional coordination weaken the ability to implement cybersecurity requirements consistently in practice.

4.2. The analysis of RQ1–RQ4 showed that the principal cybersecurity management problems in e-health arise not from isolated technical deficiencies, but from insufficient interconnection between management processes. According to the experts, the most significant factors are a clear allocation of responsibilities, coordination between the strategic, tactical, operational, and technological management levels, and consistent risk and incident management. These results provided an empirical basis for refining the model by strengthening its managerial mechanisms.

4.3. In light of the problems identified by the experts and the results of the empirical research, the conceptual model was refined, with greater emphasis placed on the managerial mechanisms of its implementation. The refined model strengthens the elements of responsibility allocation, coordination between organisational units and institutions, risk-based resource planning, incident management, feedback, and maturity assessment. These additions enable the model to be more closely aligned with practical management processes in e-health organisations and with the problems identified by the experts.

5. The expert evaluation of the refined cybersecurity management model showed that its structure is logically coherent, corresponds to the cybersecurity

management needs in e-health identified by the experts, and can be applied as a practical basis for identifying management gaps and establishing priorities for improvement.

5.1. The results of the expert interviews provided a basis for assessing the practical significance of the proposed model for cybersecurity management in e-health organisations. The experts associated the potential application of the model with clearer allocation of responsibilities, risk-based resource planning, more consistent risk and incident management, strengthened interinstitutional coordination, and more targeted improvement of cybersecurity maturity.

5.2. According to the experts, the greatest practical significance lies in the clearer allocation of responsibilities provided for in the model, the structuring of incident management, and the adaptation of management decisions to the specific characteristics of the e-health system. These elements provide a managerial basis for organising cybersecurity processes more consistently and reducing the gap identified by the experts between formal requirements and their practical implementation.

5.3. Kendall's coefficient of concordance demonstrated a high level of agreement among the experts' assessments; therefore, the results may be considered consistent within the limits of the research sample. The expert evaluation substantiated the suitability of the refined model for identifying governance fragmentation, strengthening clarity of responsibilities, and structuring the relationships between risk and incident management.

6. The results of the theoretical and empirical analyses enabled the formulation of recommendations for the application of the refined cybersecurity management model, focusing on the consistency of managerial decisions, allocation of responsibilities, risk-based resource planning, interinstitutional coordination, and periodic assessment of cybersecurity maturity. The integration of these mechanisms provides a practical basis for the systematic application of the model within the management processes of e-health organisations.

6.1. The application of the refined model is based on its integration into the principal organisational management processes, including strategic planning, allocation of responsibilities, risk and incident management, resource planning, and performance monitoring. This principle of application enables the model to be used not only to describe the state of cybersecurity, but also as a managerial instrument for identifying management gaps, substantiating priorities, and assessing changes in organisational maturity.

6.2. The developed recommendations operationalise the application of the refined model by linking its structural elements with specific managerial actions: assessment of the current state of management, priority setting, allocation of responsibilities, integration of risk and incident

management, and alignment of technological solutions with organisational management objectives. This application principle creates conditions for a more consistent assessment of cybersecurity maturity and for targeted planning of its improvement.

6.3. The practical application guidelines complement the refined model with specific implementation mechanisms and enable it to be applied as a basis for the continuous improvement of cybersecurity management. The results of model application should be assessed periodically by analysing changes in maturity, incident management indicators, the state of business continuity, and other criteria reflecting organisational preparedness. Such assessment would make it possible to determine, on a substantiated basis, the extent to which application of the model is associated with progress in cybersecurity management within the context of a specific e-health organisation.

RECOMMENDATIONS

• *Apply the refined cybersecurity management model for the improvement of the e-health system as a strategic framework for cybersecurity management within the e-health system.*

It is recommended that the refined model be used as a reference management framework to support the alignment of cybersecurity within the e-health system with the strategic objectives of healthcare digitalisation, service continuity, patient safety, and critical infrastructure protection. The model should be integrated into strategic documents at both national and organisational levels, cybersecurity policies, information security management systems, and e-health development programmes.

When applying the model, cybersecurity should not be understood as a separate technical function. Rather, it should be treated as an integrated management domain in which strategic decisions, organisational responsibilities, risk management, incident management, technological measures, and legal compliance operate as interconnected elements.

• *Use the model as a diagnostic instrument for identifying cybersecurity management gaps.*

It is recommended that the refined model be applied in assessments of the state of cybersecurity management within e-health organisations. Such assessments should cover the management levels distinguished in the model – strategic, tactical, operational, and technological – as well as the functional dimensions of risk management, incident management, allocation of responsibilities, information flow security, data protection, legal compliance, maturity assessment, and continuous improvement.

In practice, this could be implemented as a periodic self-assessment or internal audit instrument. Each organisation applying the model should assess which elements have already been implemented, which operate in a fragmented manner, and which are absent. In this way, the model would enable organisations not only to describe the current situation, but also to identify priority areas for improvement related to clarity of responsibilities, integration of risk management, preparedness for incident management, adequacy of technological measures, and organisational learning.

• *Use the model as a basis for clearly allocating responsibilities across the strategic, tactical, operational, and technological management levels.*

The results of the empirical research showed that one of the most significant problems in e-health cybersecurity management is the lack of clarity in the allocation of responsibilities and the fragmentation of governance. It is therefore recommended that the model be used as a basis for responsibility allocation. At the strategic level, management responsibility should be defined with regard to cybersecurity priorities, risk tolerance, resource allocation, and the evaluation of security indicators. At the tactical level, coordination functions, the development of policies and procedures, and mechanisms for cooperation between organisational units should be established. At

the operational level, day-to-day security processes, incident registration, response, escalation, and recovery should be clearly defined. At the technological level, specific control measures should be established for access management, monitoring, infrastructure protection, and data security. In this way, the model could be applied as a practical basis for developing a responsibility matrix.

• *Base the allocation of cybersecurity resources on risk assessment and established management priorities.*

It is recommended that decisions concerning the allocation of financial, human, and technological resources to cybersecurity be directly linked to the results of organisational risk assessments, the criticality of e-health services, and identified management gaps. In this way, resource allocation would be based not on isolated technological needs or reactive responses to incidents, but on a consistent assessment of organisational cybersecurity priorities.

When applying the refined model, senior management should periodically assess whether the available resources correspond to the identified level of risk and the selected cybersecurity objectives. This would create conditions for more targeted planning of investments, enhancement of employee competencies, implementation of technological measures, and solutions required to ensure business continuity.

• *Strengthen interinstitutional coordination of cybersecurity management within the e-health system.*

Cybersecurity within the e-health system depends on the interaction between different institutions, healthcare organisations, information system managers, and technology service providers. It is therefore recommended that interinstitutional coordination procedures, responsibilities, principles of information exchange, and actions to be taken during cyber incidents be clearly defined.

In practice, this may be implemented through permanent coordination mechanisms, common points of contact, harmonised incident escalation procedures, and periodic joint exercises. Such interaction would create conditions for faster exchange of information on risks and incidents, reduce duplication of responsibilities, and support more consistent implementation of cybersecurity requirements across the entire e-health system.

• *Integrate risk and incident management into a single coherent cycle on the basis of the model.*

It is recommended that the model be applied to link risk management, incident management, and organisational learning. Risk assessment should not be limited to the formal documentation of risks. It should be used to inform decisions regarding security priorities, financing, infrastructure renewal, access control, employee training, and incident preparedness.

In the area of incident management, the model should be applied as a process framework encompassing incident identification, registration, classification,

escalation, response, communication, service recovery, and post-incident analysis. Following each significant incident, an assessment should be conducted to determine which elements of the model functioned effectively and which require further improvement.

• *Apply the refined model to the planning and prioritisation of technological security measures.*

It is recommended that the model be used not only for managerial purposes, but also for planning technological decisions. The model should support the alignment of technological security measures with risk assessment, the organisation's maturity level, and the criticality of e-health operations. When planning technological measures, particular attention should be paid to identity and access management, user rights control, privileged user monitoring, security event monitoring, log analysis, data protection, backup management, medical device security, and the protection of inter-system integrations.

The model should also be used to assess whether technological solutions are being implemented in a fragmented manner. Technological investments should be justified not only by technical needs, but also by their impact on the overall cybersecurity management system. This would help ensure that the technological level is aligned with strategic and tactical decisions and that security measures are planned not as isolated solutions, but as elements of an integrated security architecture.

• *Integrate the model into e-health system improvement and project management processes.*

Because the model is oriented towards the design, implementation, administration, and improvement stages of the e-health system, it is recommended that it be applied not only to the security assessment of systems already in operation, but also to the planning of new e-health solutions. In every e-health development or modernisation project, the elements of the model should be used as control questions: Have responsibilities been defined? Has a risk assessment been conducted? Have incident management actions been planned? Has the security of information flows been ensured? Has a mechanism for system monitoring and continuous improvement been established?

Such application of the model would enable cybersecurity to be integrated not only after system implementation, but from the early stages of design and deployment. This is particularly important in the e-health system, where new solutions frequently involve the processing of sensitive health data, interaction between different information systems, and stringent service availability requirements.

LIST OF SCIENTIFIC PUBLICATIONS

1. Limba, T.; Lelešienė, L.; Novogreckas, S. (2022). Using WEB 2.0 and Social Networking in Education: Theoretical Insights. *EDULEARN22: 14th International Conference on Education and New Learning Technologies*, Palma, Spain, 4th–6th of July, 2022. https://doi.org/10.21125/edulearn.2022.0834
2. Limba, T.; Lelešienė, L.; Novogreckas, S. (2022). Social and Digital Media in Education. *EDULEARN22: 14th International Conference on Education and New Learning Technologies*, Palma, Spain, 4th–6th of July, 2022. https://doi.org/10.21125/edulearn.2022.1468
3. Tvaronavičienė, M.; Plėta, T.; Beretas, C. P.; Lelešienė, L. (2022). Analysis of the Critical Infrastructure Cyber Security Policy. *Insights into Regional Development,* 4(1), 26–39. https://doi.org/10.9770/ird.2022.4.1(2)
4. Katina, J.; Plėta, T.; Petkevičius, R.; Lelešienė, L. (2023). Industrial Control Systems (ICS) Cyber Prediction Model. *Insights into Regional Development,* 5(1), 86–96. https://doi.org/10.9770/ird.2023.5.1(6)
5. Limba, T.; Lelešienė, L.; Novogreckas, S.; Kowalewska, A. (2023). Knowledge and Innovation Management. *EDULEARN23: 15th International Conference on Education and New Learning Technologies,* Palma, Spain, 3rd–5th of July, 2023. https://doi.org/10.21125/edulearn.2023.0826
6. Limba, T.; Lelešienė, L.; Novogreckas, S.; Kowalewska, A. (2024). Exploring the Impact of Artificial Intelligence on Educational Paradigms: Unleashing the Potential. *EDULEARN24: 16th International Conference on Education and New Learning Technologies,* Palma, Spain, 1st–3rd of July, 2024. https://doi.org/10.21125/edulearn.2024.1087
7. Limba, T.; Lelešienė, L.; Novogreckas, S.; Kowalewska, A. (2024). Harnessing Artificial Intelligence, Chatbots and Robots for Transformative Education: Exploring the Convergence. *EDULEARN24: 16th International Conference on Education and New Learning Technologies,* Palma, Spain, 1st–3rd of July, 2024. https://doi.org/10.21125/edulearn.2024.1094
8. Limba, T.; Lelešienė, L.; Lelešius, V.; Novogreckas, S. (2025). Lessons from Large-Scale International Projects: Insights for Global Education, Collaboration, and AI Integration. *INTED2025 Proceedings: 19th International Technology, Education and Development Conference,* Valencia, Spain, 3rd–5th of March, 2025. https://doi.org/10.21125/inted.2025.1639
9. Limba, T.; Lelešienė, L.; Lelešius, V.; Novogreckas, S. (2025). Education in the Age of AI: Exploring the Role of ChatGPT, Innovations, and Future Directions. *INTED2025 Proceedings: 19th International Technology, Education and Development Conference*, Valencia, Spain, 3rd–5th of March, 2025. https://doi.org/10.21125/inted.2025.1638
10. Limba, T.; Lelešienė, L.; Lelešius, V. (2026). Cybersecurity Competence Gaps in E-Health Systems: Educational Needs Identified Through Expert Evaluation. *ICERI2026: 19th International Conference of Education, Research and Innovation,* Seville, Spain, 9th–11th of November, 2026. [Accepted for publication]

11. Limba, T.; Lelešienė, L.; Lelešius, V. (2026). Comparing Cybersecurity Approaches in European E-Health Systems: Lessons from Estonia, Finland and Denmark for Professional Education. *ICERI2026: 19th International Conference of Education, Research and Innovation,* Seville, Spain, 9th–11th of November, 2026. [Accepted for publication]

PRESENTATIONS AT SCIENTIFIC CONFERENCES

1. Limba, T.; Lelešienė, L.; Novogreckas, S. Using WEB 2.0 and Social Networking in Education: Theoretical Insights. *EDULEARN22: 14th International Conference on Education and New Learning Technologies,* Palma, Spain, 4th–6th of July, 2022.
2. Limba, T.; Lelešienė, L.; Novogreckas, S. Social and Digital Media in Education. *EDULEARN22: 14th International Conference on Education and New Learning Technologies,* Palma, Spain, 4th–6th of July, 2022.
3. Limba, T.; Lelešienė, L.; Novogreckas, S.; Kowalewska, A. Knowledge and Innovation Management. *EDULEARN23: 15th International Conference on Education and New Learning Technologies,* Palma, Spain, 3rd–5th of July, 2023.
4. Limba, T.; Lelešienė, L.; Novogreckas, S.; Kowalewska, A. Exploring the Impact of Artificial Intelligence on Educational Paradigms: Unleashing the Potential. *EDULEARN24: 16th International Conference on Education and New Learning Technologies,* Palma, Spain, 1st–3rd of July, 2024.
5. Limba, T.; Lelešienė, L.; Novogreckas, S.; Kowalewska, A. Harnessing Artificial Intelligence, Chatbots and Robots for Transformative Education: Exploring the Convergence. *EDULEARN24: 16th International Conference on Education and New Learning Technologies,* Palma, Spain, 1st–3rd of July, 2024.
6. Limba, T.; Lelešienė, L.; Lelešius, V.; Novogreckas, S. Lessons from Large-Scale International Projects: Insights for Global Education, Collaboration, and AI Integration. *INTED2025: 19th International Technology, Education and Development Conference,* Valencia, Spain, 3rd–5th of March, 2025.
7. Limba, T.; Lelešienė, L.; Lelešius, V.; Novogreckas, S. Education in the Age of AI: Exploring the Role of ChatGPT, Innovations, and Future Directions. *INTED2025: 19th International Technology, Education and Development Conference,* Valencia, Spain, 3rd–5th of March, 2025.
8. Limba, T.; Lelešienė, L.; Lelešius, V. Cybersecurity Competence Gaps in E-Health Systems: Educational Needs Identified Through Expert Evaluation. *ICERI2026: 19th International Conference of Education, Research and Innovation,* Seville, Spain, 9th–11th of November, 2026.
9. Limba, T.; Lelešienė, L.; Lelešius, V. Comparing Cybersecurity Approaches in European E-Health Systems: Lessons from Estonia, Finland and Denmark for Professional Education. *ICERI2026: 19th International Conference of Education, Research and Innovation,* Seville, Spain, 9th–11th of November, 2026.

CURRICULUM VITAE

Education

2020 – 2026	Doctoral Student in Management, Mykolas Romeris University
2018 – 2020	Master of Cyber Security Management, Mykolas Romeris University

Professional Experience

Since 2023	Head of the Information Technology Division, State Data Protection Inspectorate
Since 2022	Lecturer, Mykolas Romeris University
Since 2024	Practitioner Lecturer, Vilnius University Business School
2020 – 2023	Specialist, National Cyber Security Centre

Lelešienė, Lina

KIBERNETINIO SAUGUMO VALDYMO MODELIO E. SVEIKATOS SISTEMOS TOBULINIMUI VERTINIMAS: daktaro disertacija. – Vilnius: Mykolo Romerio universitetas, 2026. P. 274.

Bibliogr. 166-183 p.

Disertacijoje nagrinėjamas kibernetinio saugumo valdymas e. sveikatos sistemos kontekste, akcentuojant vadybinių, organizacinių, procesinių ir technologinių veiksnių sąveiką. Tyrimo tikslas – parengti kibernetinio saugumo valdymo modelį e. sveikatos sistemos tobulinimui ir ekspertiniu požiūriu įvertinti jo tinkamumą bei praktinio taikymo galimybes. Atlikta mokslinės literatūros, tarptautinių standartų, teisės aktų, kibernetinių incidentų ir atakų sisteminė analizė. Empiriniame tyrime taikyti pusiau struktūruoti ekspertiniai interviu, teminė analizė ir Kendall konkordacijos koeficientas W. Tyrimo rezultatai parodė, kad pagrindinės e. sveikatos kibernetinio saugumo valdymo problemos siejamos su valdymo fragmentacija, nepakankamai aiškiu atsakomybių paskirstymu, ribota skirtingų valdymo lygmenų sąveika ir nepakankamu rizikų bei incidentų valdymo integravimu. Remiantis teorinės ir empirinės analizės rezultatais, patikslintas modelis, integruojantis strateginį, taktinį, operacinį ir technologinį valdymo lygmenis. Taip pat parengta kibernetinio saugumo valdymo brandos vertinimo metodika ir praktinė vertinimo matrica, sudaranti pagrindą valdymo spragoms nustatyti ir prioritetinėms tobulinimo kryptims pagrįsti.

The dissertation examines cybersecurity management in the context of the e-health system, emphasising the interaction of managerial, organisational, process-related, and technological factors. The aim of the research is to develop a cybersecurity management model for the improvement of the e-health system and to evaluate its suitability and potential for practical application from an expert perspective. A systematic analysis of scientific literature, international standards, legal acts, cyber incidents, and attacks was conducted. The empirical research employed semi-structured expert interviews, thematic analysis, and Kendall's coefficient of concordance W. The results showed that the main problems of cybersecurity management in e-health are associated with governance fragmentation, insufficiently clear allocation of responsibilities, limited interaction between management levels, and insufficient integration of risk and incident management. Based on the theoretical and empirical findings, the model was refined to integrate strategic, tactical, operational, and technological management levels. A cybersecurity management maturity assessment methodology and a practical assessment matrix were also developed to support the identification of management gaps and the substantiation of priority areas for improvement.

Lina Lelešienė

KIBERNETINIO SAUGUMO VALDYMO MODELIO E. SVEIKATOS SISTEMOS TOBULINIMUI VERTINIMAS

Daktaro disertacija
Socialiniai mokslai, vadyba (S 003)

Mykolo Romerio universitetas
Ateities g. 20, Vilnius
Puslapis internete www.mruni.eu
El. paštas roffice@mruni.eu
Tiražas 20 egz.

Parengė spaudai MB „Arhela“

Spausdino UAB „Ciklonas“
Žirmūnų g. 68, LT-09124, Vilnius
El. p. info@ciklonas.lt
https://ciklonas.lt/