MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

ALINA PARNARAUSKIENĖ

X INFORMACINĖS SISTEMOS VERTINIMAS KIBERNETINIO SAUGUMO ASPEKTU

Magistro baigiamasis darbas

Vadovas
Dr. A. Jurgelevičius

VILNIUS, 2023

MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

X INFORMACINĖS SISTEMOS VERTINIMAS KIBERNETINIO SAUGUMO ASPEKTU

Kibernetinio saugumo valdymo magistro baigiamasis darbas

Studijų programa 6211LX066

Vadovas

Dr. A. Jurgelevičius

2023 05-02

Recenzentas

2023-05

Atliko

KSVvmis21-1 gr. stud.

A. Parnarauskienė

2023 04

VILNIUS, 2023

TURINYS

TURINYS....2
SANTRUMPOS IR TERMINAI....6
ĮVADA....8
1. INFORMACINĖS SISTEMOS KIBERNETINIO SAUGUMO VERTINIMO TEORINIAI ASPEKTAI....12
1.1. Informacinės sistemos, informacinės sistemos saugumo, kibernetinio saugumo ir informacinės sistemos kibernetinio saugumo sampratų sąsajos. 12
1.2. Informacinės sistemos kibernetinio saugumo vertinimo proceso apimtis. 16
1.3. Informacinės sistemos kibernetinio saugumo vertinimui taikomi moksliniai gerosios praktikos metodai....22
1.3.1.ISO 27001 standarto metodas....22
1.3.2.NIST CSF standarto metodas....25
1.3.3.CIS Controls standarto metodas....29
1.3.4.Gerosios praktikos metodų palyginimas. 31
1.3.5. Lietuvos teisės aktuose nustatytų reikalavimų, taikomų informacinių sistemų kibernetinio saugumo vertinimo procesui, analizė....33
2. INFORMACINĖS SISTEMOS KIBERNETINIO SAUGUMO VERTINIMO TYRIMO METODOLOGIJA....37
2.1. Tyrimo objekto pristatymas. 37
2.2. Tyrimo tikslingumo pagrindimas....38
2.3. Kokybinio tyrimo metodų pagrindimas ir apibūdinimas. 39
2.4. Tyrimo dizainas ir rezultatų patikimumas. 43
3. INFORMACINĖS SISTEMOS KIBERNETINIO SAUGUMO VERTINIMO MODELIO FORMAVIMAS....48
3.1. Informacinės sistemos kibernetinio saugumo vertinimo modelio formavimo teorinės prielaidos....48
3.2. Empirinio tyrimo ekspertų charakteristika ir apklausos klausimynų turinys....51
3.3. Ekspertinės apklausos duomenų analizė ir interpretacija. 52
3.4. Empirinio tyrimo apibendrinti rezultatai....62
3.5. Patikslintas informacinės sistemos kibernetinio saugumo vertinimo modelis....64
IŠVADOS IR PASIŪLYMAI....66
LITERATŪROS SĄRAŠAS....69
ANOTACIJA....74
SANTRAUKA....76
PRIEDAI....78

PAVEIKSLŲ SĄRAŠAS

1 pav. Informacinės sistemos gyvavimo ciklo etapai 14
2 pav. Informacijos saugumo tikslų triada (CIA modelis)....17
3 pav. Informacijos saugumo valdymo ir tobulinimo ciklas (PDCA metodas)....24
4 pav. sąrašas Rizikos valdymo gyvavimo ciklo funkcijų ir kiekvienai funkcijai priskirtų kategorijų 26
5 pav. Kategorijos ir subkategorijos su informacinėmis nuorodomis sąrašo pavyzdys 27
6 pav. Organizacijos brandumo (požiūrio į rizikas) lygio vertinimo pavyzdys....28
7 pav. 18 kibernetinei gynybai skirtų saugumo kontrolės priemonių sąrašas 30
8 pav. 2021 m. geriausios praktikos informacinių sistemų kibernetiniam saugumui vertinti 31
9 pav. 2019 m. geriausios praktikos informacinių sistemų kibernetiniam saugumui vertinti 32
10 pav. Tyrimų loginė seka ir jų dermė....44
11 pav. Informacinės sistemos kibernetinio saugumo vertinimo modelio struktūra....50
12 pav. Objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelis....65

LENTELIŲ SĄRAŠAS

1 lentelė ENISA kibernetinio saugumo specialistų rolių sąrašas.....21
2 lentelė Teisės aktų, reglamentuojančių valstybės informacinių sistemų, jose tvarkomos elektroninės informacijos saugumą ir kibernetinį saugumą, sąrašas.....34
4 lentelė Kokybinio tyrimo (ekspertų apklausos) eiga.....44
5 lentelė Mokslinių straipsnių paieškai naudotų raktinių žodžių, straipsnių pavadinimų, jų publikavimo metų sąrašas.....46
6 lentelė Informacija apie ekspertų patirtį ir atsakymų į apklausos klausimynus pateikimo datas...51
7 lentelė Iš dalies struktūruotos ekspertinės apklausos kokybinio turinio (anlg. *Content*) analizė...53
8 lentelė Privalomų informacinių sistemų kibernetinio saugumo elementų, informacijos saugumo valdymo elementų, organizacinių ir techninių priemonių kategorijų bei kibernetinei gynybai skirtų saugumo kontrolės priemonių palyginimas.....82
9 lentelė Informacija apie Registrų ir valstybės informacinių sistemų registre registruotus objektus, jų valdytojus.....84

SANTRUMPOS IR TERMINAI

ARSIS – Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistema.

CIS (angl. *The Center for Internet Security, Inc.*) – ne pelno organizacija, atsakinga už CIS Controls, CIS Benchmarks visame pasaulyje pripažintą geriausią informacinių technologijų sistemų ir duomenų apsaugos praktiką (CIS oficialus internetinis puslapis: https://www.cisecurity.org/).

COBIT (angl. *Control Objectives for Information and related Technologies*) – Informacinių technologijų valdymo ir vadovavimo metodika

CSC (angl. *Critical Security Controls*) – saugumo kontrolės priemonių rinkinys, skirtas efektyviai kibernetinei gynybai.

CSIRT (angl. *Computer Security Incident Response Team*) – kibernetinio saugumo incidentų reagavimo komanda.

CSIRT SF (angl. *Computer Security Incident Response Team Services framework*) **–** tai FIRST (angl. *Forum of Incident Response and Security Teams)* bendruomenės ir Tarptautinės telekomunikacijų sąjungos (angl. *Telecommunications Union, ITU*) sukurta struktūrizuota kibernetinio saugumo incidentų reagavimo komandos paslaugų metodika, padedanti išgryninti kokias paslaugas turi teikti kibernetinio saugumo incidentų reagavimo komanda.

Gartner įmonė (angl. *Gartner research and advisory company*) – tai tyrimus ir patarimus teikianti įmonė, kuri nagrinėja technologines tendencijas, priemones, reikalingas įgyvendinti svarbius įmonės tikslus, siekiant kurti ateities įmones.

ENISA (angl. *European union agency for cybersecurity*) – Europos Sąjungos kibernetinio saugumo agentūra, kurios tikslas – siekti aukšto bendro kibernetinio saugumo lygio visoje Europoje (ENISA oficialus internetinis puslapis: https://www.enisa.europa.eu).

FIRST (angl. *Forum of Incident Response and Security Teams*) – tai reagavimo į incidentus ir saugumo komandų forumas, vienijantis tarptautines mokslines, vyriausybines, karines ir komercines saugumo ir reagavimo į incidentus komandas. FIRST teikia mokslu ir praktika pagrįstas bendradarbiavimo platformas, metodines rekomendacijas, technologinius įrankius, padedančius reaguojanti į incidentus (FIRST oficialus internetinis puslapis: https://www.first.org/).

IEC (angl. *International Electrotechnical Commission*) – tarptautinė elektrotechnikos komisija, pasaulinė organizacija, kurianti ir skelbianti tarptautinius elektros inžinerijos, elektronikos, ryšių technologijų ir susijusių sričių standartus. IEC tvarko atitikties vertinimo schemas, kurios patvirtina, ar prietaisas, sistema ar komponentas atitinka tarptautinius standartus (IEC oficialus internetinis puslapis: https://www.iec.ch/homepage).

ISO (angl. *International Organization for Standardization*) – tarptautinė standartizacijos organizacija, kuri kuria ir skelbia tarptautinius standartus, reikalavimus, praktikas, specifikacijas. Standartų tikslas – užtikrinti gaminių, paslaugų, sistemų kokybę, saugą bei efektyvumą (ISO oficialus internetinis puslapis: https://www.iso.org/).

ISACA (angl. *Information Systems Audit and Control Association*) – tarptautinė informacinių sistemų valdymo ir audito asociacija, kuri orientuojasi į informacinių technologijų valdymą (ISACA oficialus internetinis puslapis: https://www.isaca.org).

JRC (angl. *Joint Research Centre*) – Jungtinis tyrimų centras, Europos Komisijos generalinis direktoratas, atsakingas už inovacijas, mokslinius tyrimus, teikiantis nepriklausomas, įrodymais pagrįstas mokslines ataskaitas. JTC glaudžiai bendradarbiauja su mokslinių tyrimų organizacijomis valstybėse narėse, Europos Sąjungos institucijomis ir agentūromis bei su mokslo partneriais Europoje ir tarptautiniu mastu, įskaitant Jungtinių Tautų institucijas (JRC oficialus internetinis puslapis:https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/joint-research-centre_en).

Kibernetinė erdvė – „aplinka, kurią sudaro kompiuteriai ir kita ryšių ir informacinių technologijų įranga ir juose sukuriama ir (arba) jais perduodama elektroninė informacija“ (Lietuvos Respublikos Kibernetinio saugumo įstatymas, 2018)

NIST (angl. *The National Institute of Standards and Technology*) – Jungtinių amerikos valstijų (toliau – JAV) Nacionalinis standartų ir technologijų institutas, JAV prekybos departamento dalis. NIST yra viena iš seniausių fizinių mokslų laboratorijų JAV, kurianti standartus, skirtus technologiniam ir ekonominiam saugumui užtikrinti (NIST oficialus internetinis puslapis: https://www.nist.gov/).

NKSC (angl. NCSC) – Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (angl. National Cyber Security Centre under the Ministry of Defence).

Pasaulinis kibernetinio saugumo pajėgumų centras (angl. *Global Cyber Security Capacity Centre*) – tai Oxfordo universiteto pirmaujantis tarptautinis veiksmingo ir efektyvaus kibernetinio saugumo pajėgumų didinimo tyrimų centras, skatinantis kibernetinio saugumo pajėgumų stiprinimo iniciatyvų mastą, kokybę ir poveikį visame pasaulyje (oficialus GCSCC internetinis puslapis https://gcscc.ox.ac.uk/about-us).

SANS institutas (angl. *SysAdmin Audit, Networking and Security Institute*) – privati Jungtinių amerikos valstijų pelno siekianti įmonė, įkurta 1989 m., kuri specializuojasi informacijos saugumo, kibernetinio saugumo mokymų srityse. Mokymų temos apima kibernetinę ir tinklo apsaugą, pažeidžiamumų testavimus, reagavimą į incidentus, skaitmeninę teismo ekspertizę ir auditą (SANS oficialus internetinis puslapis: https://www.sans.org/emea/).

ĮVADAS

Temos aktualumas. Skaitmeninės technologijos – neatsiejama kiekvienos valstybės informacinės infrastruktūros dalis. Visos strateginės sritys yra priklausomos nuo tarpusavyje susijusių tinklų ir informacinių sistemų, jų kibernetinis saugumas vis labiau tampa kiekvienos valstybės nacionalinio saugumo klausimas. Kibernetinis grėsmės nuolat išnaudoja informacinių sistemų sudėtingumą, jungiamumą su ypatingos svarbos infrastruktūra, keldamos pavojų jų saugumui, organizacijų veiklai, visuomenės ir nacionaliniam saugumui. Nesuvaldytos kibernetinio saugumo rizikos didina išlaidas krizės atveju. Ponemon instituto (angl. *Ponemon Institute*) ir IBM Security 2022 m. atlikto mokslinio tyrimo duomenimis išlaidos, kurias pasaulio valstybės patiria dėl duomenų saugumo pažeidimų nuo 2020 m. kasmet tik didėja. 2022 m. Pasaulio ekonomikos forume pristatytoje globalios rizikos ataskaitoje pažymima, kad kibernetinio saugumo grėsmės nuo 2020 m. kelia ir per artimiausius 10 m. kels didžiausią riziką visuomenės saugumui. Dėl didėjančių išorinių ir vidinių grėsmių, organizacijoms būtina turėti nuoseklų, sisteminį, kartotinį ir visuminį (holistinį) požiūrį į kibernetinio saugumo valdymą, informacinių sistemų saugumą neatsižvelgiant į informacinės sistemos sudėtingumą, organizacijos dydį, organizacijai ar valstybei kylančias grėsmes.

Mokslinė problema ir tyrimo aktualumas. Informacinių sistemų kibernetinio saugumo, atitikties kibernetinio saugumo reikalavimams vertinimo aspektai nagrinėjami tiek Lietuvos tiek užsienio mokslininkų. Akademinė bendruomenė, tarptautinės organizacijos, Pasaulinis kibernetinio saugumo pajėgumų centras nuolat rengia įvairius modelius, skirtus valstybėms, organizacijoms pasirengti grėsmėms kibernetinėje erdvėje (Baldini G., Barrero J., 2020). Sutinkama, kad jokia organizacija negali tikėtis, kad jos informacinės sistemos 100% atitiks kibernetinio saugumo reikalavimus, tačiau būtina to siekti, nes baudos už tokių reikalavimų nesilaikymą, duomenų praradimą gali pakenkti organizacijai, sukelti bankrotą (Harris M. A., 2021). Tarptautiniai standartai ir metodai yra tvirtas pagrindas atlikti objektyvius informacinių sistemų kibernetinio saugumo vertinimus, vadovaujantis gerąja praktika, tiek kritinės infrastruktūros valdytojams (Roshanaei M., 2021) tiek mažoms ir vidutinėms įmonėms (Venkatesh V., 2018), jie pritaikomi ir kuriant nacionalines kibernetinio saugumo sistemas (Angelini M., Ciccotelli C., 2020). Taikant gerosios praktikos metodus, kibernetinio saugumo vertinimo procesas gali būti veiksmingas norint atrasti informacijos saugumo valdymo problemas organizacijos viduje, siekiant nustatyti esamus kibernetinio saugumo trūkumus, įvertinti kaip organizacijos laikosi kibernetinio saugumo įsipareigojimų (pvz. nustatytų teisės aktuose). Siekiančios kibernetinės brandos organizacijos taiko tarptautinių standartizacijos organizacijų siūlomus metodus, tačiau pasaulinėje praktikoje ir Lietuvoje egzistuoja neatitikties (angl. *noncompliance*) problematika arba kitaip dar vadinama formaliąja atitiktimi (Štitilis D., 2021).

Periodiniai atitikties vertinimai ir auditai – pagrindinis būdas įvertinti organizacijos, jos informacinių sistemų, kibernetinį saugumą, nustatyti neatitiktis (Jadhav K., 2020). Lietuvoje valstybės informacinių sistemų, ypatingos svarbos informacinės infrastruktūros (toliau – YSII) valdytojų atitikties teisės aktuose nustatytiems kibernetinio saugumo reikalavimams vertinimą, priežiūrą ir stebėseną atlieka NKSC. 2020 m. NKSC atlikus atitikties vertinimus, buvo nustatyta, kad tik pusė visų organizacijų vadovaujasi informacinių sistemų saugos dokumentuose nustatytais saugumo reikalavimais (Nacionalinė kibernetinio saugumo būklės ataskaita, 2021). NKSC pateikti rezultatai parodė aplaidų informacinių sistemų valdytojų ir tvarkytoju požiūrį į kibernetinio saugumo reikalavimų įgyvendinimą. Analizuojant 2016-2021 m. nacionalinės kibernetinio saugumo būklės ataskaitas pastebėta, kad tok aplaidus, formalus, nebrandus požiūris į kibernetinio saugumo reikalavimų įgyvendinimą nekinta nuo 2016 m. Apie nepakitusį kibernetinio saugumo brandos lygį pažymima ir 2022 m. Nacionalinėje kibernetinio saugumo būklės ataskaitoje. 2022 m. atlikto valstybinio audito ataskaitoje „Kibernetinis saugumo užtikrinimas“ (toliau – Valstybinio audito ataskaita) nurodoma, kad nuo 2019 m. beveik pusė informacinių išteklių valdytojų ir tvarkytojų nė karto neatliko informacinių technologijų saugos atitikties vertinimo. Apie organizacijų nesirūpinimą savo informacinių sistemų kibernetiniu saugumu pažymima ir 2020 m. visuomenei pristatytoje 2021-2027 m. Visuomenės skaitmeninimo išankstinio poveikio vertinimo ataskaitoje.

Analizuojant mokslines teorijas pastebėta, kad neatitikties kibernetinio saugumo reikalavimams priežastys gali slypėti pačiame informacinės sistemos kibernetinio saugumo vertinimo procese. Daugelis mokslininkų pažymi, kad informacinės sistemos kibernetinio saugumo vertinimo procesas susijęs su įvairiomis sritimis, techniniais, teisiniais, finansų, vadybos klausimais ir žmogaus elgesiu. Pagal Leger M. A. visa tai prisideda prie proceso subjektyvumo didinimo ir žmogiškųjų klaidų, ypač tuo atveju, kai nėra holistinio požiūrio į kibernetinį saugumą (Leger M. A., 2022). Mokslininkai tyrinėja skirtingus faktorius, turinčius įtakos informacinių sistemų kibernetiniam saugumui, pvz. organizacijų kontekstą (politiką, procesus, darbo kultūrą) (Marotta A., Madnick S., 2021), informacinių ir pramoninių sistemų projektavimo spragas (Qassim Q., Jamil N., 2019), technologinį pažeidžiamumą (Fathi S., Hikal N., 2019), žmogiškuosius veiksnius (Harrel M.N, 2014), teisės aktuose nustatyto teisinio reglamentavimo įtaką organizacijos kibernetiniam saugumui (Al-hashimi, M., Othman, 2018, Štitilis D., Pakutinskas P., 2011) ir kt. Tačiau atsakymų dėl kokių priežasčių atsiranda neatitikties apraiškos vis dar ieškoma. Dalis mokslininkų mano, kad tik sukūrus veiksmingą informacinės sistemos kibernetinio saugumo vertinimo modelį, galima būtų objektyviai atlikti informacinės sistemos kibernetinio saugumo vertinimą (Harris M.A., 2021). Tokio modelio sukūrimas galėtų išspręsti formalaus informacinės sistemos kibernetinio saugumo vertinimo problemą ateityje. Tačiau šiuo metu ši problema neturi sprendimo.

Mokslinė darbo vertė ir mokslinis darbo naujumas. Holistinis požiūris į informacinių sistemų kibernetinio saugumo vertinimo procesą yra būtinas. Šiame darbe, taikant tokį požiūrį, yra kuriamas objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelis, išgryninami pagrindiniai vertinimo proceso elementai, identifikuojama vertinimo imtis (veiklos ir priemonės), vertinimo problematika, neatitikties (formalios atitikties) atsiradimo priežastys, pasiūlomos gerinimo priemonės. Darbu daromas mokslinis indėlis gerinant organizacijų, jų valdomų informacinių sistemų kibernetinio saugumo būklę, formuojamos prielaidos tolimesniam šios temos tyrinėjimui.

Praktinė darbo reikšmė. Darbas atskleidžia egzistuojančias informacinių sistemų kibernetinio saugumo vertinimo problemas, pasiūlo būdus joms spręsti. Darbu siekiama keisti ydingą neatitikties (formalios atitikties) praktiką. Organizacijos informacinių sistemų kibernetinio saugumo vertinimus privalo atlikti objektyviai ir taip siekti atitikties teisės aktuose nustatytiems kibernetinio saugumo reikalavimams. Tačiau praktiškai nėra metodų, rekomendacijų, aprašančių, kaip toks vertinimas turėtų būti atliekamas. Šiame darbe sukurtas informacinės sistemos kibernetinio saugumo vertinimo modelis gali būti taikomas praktikoje organizacijų, siekiančių objektyviai atlikti informacinių sistemų kibernetinio saugumo vertinimus, siekiančių atitikties kibernetinio saugumo reikalavimams visuose organizacijos kibernetinio saugumo valdymo lygmenyse.

Tyrimo problema. Kaip, taikant šiuolaikinius mokslinius ir gerosios praktikos metodus objektyviai atlikti informacinės sistemos kibernetinio saugumo vertinimą?

Tyrimo objektas: informacinės sistemos kibernetinio saugumo vertinimo procesas.

Tyrimo dalykas: informacinės sistemos kibernetinio saugumo vertinimo proceso, kaip reiškinio, analizė pasitelkiant teorines, teisines, mokslines informacinių sistemų kibernetinio saugumo vertinimo strategijas, gerosios praktikos metodus ir praktinius šio proceso įgyvendinimo aspektus.

Tyrimo tikslas: sukurti informacinės sistemos kibernetinio saugumo vertinimo modelį ir pateikti rekomendacijas objektyviam informacinių sistemų kibernetinio saugumo vertinimui atlikti.

Tyrimo uždaviniai:

1. Išanalizuoti mokslinę literatūrą, teorines strategijas, mokslinius tyrimus, tarptautinę gerąją praktiką, Europos Sąjungos, Lietuvos tesės aktuose nustatytus reikalavimus, metodus, taikomus informacinių sistemų kibernetinio saugumo vertinimo procesui, palyginti jų privalumus ir trūkumus, identifikuoti vertinimo proceso imtį, problematiką.
2. Sukurti informacinės sistemos kibernetinio saugumo vertinimo modelį.
3. Atlikti kokybinį tyrimą, kurio pagrindu galima būtų įvertinti sukurtą modelį, identifikuoti neatitikties (formalios atitikties) atsiradimo priežastis, numatyti (pasiūlyti) gerinimo priemones.
4. Įvertinti sukurto informacinės sistemos kibernetinio saugumo vertinimo modelio taikymo praktikoje galimybes, pateikti siūlymus dėl objektyvaus informacinės sistemos kibernetinio saugumo vertinimo proceso tobulinimo krypčių.

Duomenų rinkimo metodai:

1. Sisteminė mokslinės literatūros, mokslinių tyrimų, gerosios praktikos metodų, Europos sąjungos ir Lietuvos Respublikos teisės aktų, valstybės informacinių sistemų saugos politiką reglamentuojančių juridinių ir kitų dokumentų turinio analizė (angl. *Content analysis*).
2. Atvejo analizė (angl. *Case study*).
3. Ekspertinė kokybinė apklausa.

Duomenų analizės metodai:

1. Kokybinė dokumentų turinio (angl. *Content*), pirminių ir antrinių duomenų analizė.
2. Ekspertinės kokybinės apklausos turinio (angl. *Content*) analizė ir interpretavimas.
3. Sisteminė kokybinė gautų duomenų analizė (tyrimo rezultatų ir pasiūlymų pateikimas).

Darbo struktūra. Darbą sudaro 3 skyriai. Pirmame skyriuje analizuojami informacinės sistemos kibernetinio saugumo vertinimo teoriniai aspektai ir problematika. Antrame skyriuje pateikiama tyrimo metodologija, identifikuojami empirinio tyrimo dalyviai, duomenų rinkimo šaltiniai, duomenų rinkimo metodai, kokybinio tyrimo duomenų patikimumo užtikrinimo būdai. Trečiame skyriuje pateikiamas teoriniu pagrindu sukurtas ir empiriniu tyrimu pagrįstas objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelis, identifikuojamos neatitikties (formalios atitikties) atsiradimo priežastys, pasiūlomos gerinimo priemonės ir pateikiami siūlymai dėl objektyvaus informacinės sistemos kibernetinio saugumo vertinimo proceso tobulinimo krypčių.

1. INFORMACINĖS SISTEMOS KIBERNETINIO SAUGUMO VERTINIMO TEORINIAI ASPEKTAI

1.1. Informacinės sistemos, informacinės sistemos saugumo, kibernetinio saugumo ir informacinės sistemos kibernetinio saugumo sampratų sąsajos.

Informacinėms sistemoms, jų saugumo vertinimui mokslinėje literatūroje skiriama nemažai dėmesio. Dėl mokslinių tyrimų ir nagrinėjamos problematikos įvairovės egzistuoja daugybė informacinių sistemų apibrėžimų:

1. „Informacinė sistema, automatizuota arba rankinė sistema, skirta rinkti, kaupti, saugoti, koreguoti, apdoroti, perduoti, pateikti informaciją. Ją sudaro žmonės, techninė įranga (kompiuteriai, jų tinklai, ryšio priemonės), duomenų bazės, programinė įranga“ (Lietuvos visuotinėje enciklopedija, 2005).

2. „Informacinė sistema – tai žmonių, funkcijų ir technologijų sistema“ (Mikalauskienė A., Brazaitis Z., 2006).

3. „Informacinė sistema – tai informacijos apdorojimo sistemos ir organizacijos išteklių (organizacijos informacijos, žmonių, techninių priemonių, finansų ir panašiai) visuma, skirta informacijai formuoti (kurti) ir skleisti“ (Simanauskas L., 2000).

4. „Informacinė sistema – tai dažniausiai automatizuota sistema, kurią sudaro žmonės, kompiuteriai ir kita įranga, metodai ir priemonės rinkti, apdoroti, saugoti, perduoti duomenis, o iš jų pateikti informaciją vartotojams. Informacija – tai duomenys, apdoroti taip, kad turėtų prasmę ir būtų naudingi vartotojui, o duomenys yra tik faktai apie tam tikrus įvykius ar aplinkos reiškinius, jie yra žaliava informacijai gauti“ (Trček D., 2006).

5. „Informacinė sistema – tai komponentų kompleksas įvairių rūšių duomenims ir informacijai rinkti, išsaugoti, apdoroti, laikyti ir skleisti siekiant tam tikrų organizacijos tikslų ir taikant kompiuterines technologijas“ (Dzemydienė D., Naujikienė R, 2004, Patašienė I., Zaukas G., 2015).

Siaurąją prasme informacinė sistema suprantama kaip iš vieno ar kelių kompiuterių, įvairių išorinių įrenginių ir programinės įrangos sudaryta, informacinių technologijų pagrindu veikianti infrastruktūra, skirta informacijai apdoroti, įskaitant elektroninių ryšių tinklus, kuriais perduodama informacija (duomenys). Plačiąja prasme informacinė sistema suprantama kaip informacinių technologijų pagrindu veikianti sistema, funkcionuojanti organizacijos veiklos aplinkoje, apimanti organizacijos išteklius (techninius, finansinius, organizacinius, žmogiškuosius) ir kurios tikslas sudaryti sąlygas automatizuoti tam tikrus organizacijos funkcinius procesus, automatizuotai tvarkyti informaciją, ją skleisti.

Informacinėse sistemose apdorojama skirtingo lygio informaciją, tiek viešo tiek ne viešo pobūdžio. Priklausomai nuo informacijos, kuri apdorojama informacinėje sistemoje svarbos (lygio, kategorijos), nustatoma informacinės sistemos svarba (lygis, kategorija), parenkamas lygiavertis ir proporcingas informacijos, informacinės sistemos saugumo lygis. Kadangi šiame darbe sukurtas informacinės sistemos kibernetinio saugumo vertinimo modelis bus tikrinamas informacinių sistemų, kurios, pagal informacijos, tvarkomos jose svarbą, yra priskirtos valstybės informacinėms sistemoms, atžvilgiu, vertėtų paminėti kokios informacinės sistemos laikytinos valstybinėmis. Valstybės informacinių išteklių valdymo įstatymo 2 straipsnio 14 punkte nustatyta, kad valstybės informacinė sistema – tai „valstybės institucijai (institucijoms) ar valstybės įstaigai (įstaigoms) teisės aktų nustatytoms funkcijoms, išskyrus vidaus administravimą, atlikti reikalingą informaciją apdorojanti teisinių, organizacinių, techninių ir programinių priemonių visuma“. Pagrindinis požymis, skiriantis informacinę sistemą nuo valstybinės – tai informacijos (duomenų), kuri yra kaupiama ir tvarkoma informacinėje sistemoje svarba. Valstybės informacinėse sistemose ji yra susijusi su valstybės institucijos, įstaigos, įmonės veikla, teisės aktuose pavestomis atlikti funkcijomis.

Kadangi šiame darbe informacinės sistemos nagrinėjamos kibernetinio saugumo aspektu, verta pažymėti, kad mokslinėje literatūroje dažnai vartojami du terminai informacinių sistemų saugumui apibūdinti: *informacinių sistemų saugumas* ir *informacinių sistemų apsauga.* Terminai *saugumas* ir *apsauga* dažnai vartojami tai pačiai sąvokai apibūdinti, tačiau tai visiškai skirtingos sąvokos. Pagal gerosios praktikos šaltinius (pvz. ISO/IEC 27000 standartą) informacinės sistemos saugumas turėtų būti suprantamas kaip organizacijos informacijos, informacinės sistemos, kaip turto, konfidencialumo, vientisumo ir prieinamumo užtikrinimas viso šio turto gyvavimo ciklo metu. Kai kuriuose moksliniuose šaltiniuose nurodoma, kad informacinės sistemos saugumas „tai tokia sistemos būklė, kai sistema sugeba atlaikyti destabilizuojantį vidinių ir išorinių grėsmių poveikį, kai sistemos funkcionavimas nesukelia grėsmių jai pačiai ir išorinei aplinkai“ (Mikalauskienė A., Brazaitis Z., 2006). Iš esmės informacinės sistemos saugumas gali būti apibūdinamas kaip būsena, kuomet negalima padaryti žalos informacinės sistemos ir (ar) jos komponentų savybėms arba jų veiklai, t.y. būsena, kai nėra rizikų, kurios galėtų sukelti žalą informacinei sistemai, o jeigu tokios ir yra, jos yra suvaldytos taip, kad jokios grėsmės informacinės sistemos saugumui (konfidencialumui, vientisumui ir prieinamumui) nėra (Idrisov H., 2020). Informacinių sistemų saugumo valdymas, kaip procesas, siejamas su informacijos, informacinės sistemos gyvavimo ciklu (Kissel R., Stine K., 2019). Informacinės sistemos saugumo užtikrinimas visais atvejais yra suprantamas kaip procesas, kurio metu informacijos saugumas valdomas (užtikrinamas) nuo sumanymo (koncepcijos) kurti informacinę sistemą iki informacinės sistemos veikimo pabaigos (Dzemydienė D., Naujikienė R, 2004). Informacinės sistemos gyvavimo ciklo etapai pavaizduoti 1 paveiksle.



1 pav. Informacinės sistemos gyvavimo ciklo etapai

Šaltinis: parengta šio darbo autorės pagal Pritaikytosios ir standartizuotosios duomenų apsaugos informacinės sistemos gyvavimo ciklo gaires, prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Pritaikytoji_ir_standartizuotoji_apsauga_IS_gyvavimo_cikle_2020-12.pdf

Sąvoka *informacinės sistemos apsauga* mokslinėje literatūroje vartojama tuomet, kai nagrinėjami metodai ir priemonės, kurios taikomos informacinės sistemos saugumui užtikrinti. Pažymėtina, kad Lietuvos nacionalinėje teisėje (pvz., Valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše) dažnai vartojamas dar vienas terminas *informacinės sistemos sauga*. Terminas *sauga* mokslinėje literatūroje vartojamas apibūdinant priemones, užtikrinančias, kad nekiltų rizikos, galinčios sukelti grėsmę, pavojų informacijai, kaip objektui. Todėl dažnu atveju kai nagrinėjama informacinės sistemos apsauga ir informacinės sistemos sauga, tai reiškia tą patį – priemonių (organizacinių ir techninių) ir metodų (būdų), skirtų informacinės sistemos saugumui užtikrinti, taikymą.

Europos Sąjungos ir Lietuvos nacionalinėje teisėje vartojamos skirtingos informacinių sistemų saugumą apibūdinančios sąvokos. Pavyzdžiui, 2022 m. gruodžio 14 d. Europos parlamento ir Tarybos direktyvoje (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 direktyvoje (toliau – TIS 2 direktyva) vartojama sąvokos *tinklai ir informacinės sistemos, tinklų ir informacinių sistemų saugumas*. Pagal Europos Sąjungos teisinį reglamentavimą tinklų ir informacinių sistemų saugumas apibrėžiamas kaip „tinklų ir informacinių sistemų pajėgumas tam tikru patikimumo lygiu išlikti atspariems bet kokiam įvykiui, galinčiam sukelti pavojų saugomų, perduodamų ar tvarkomų duomenų, arba teikiamų ar per tas tinklų ir informacines sistemas gaunamų paslaugų prieinamumui, autentiškumui, vientisumui ar konfidencialumui“ (žr. TIS 2 direktyvos 6 straipsnio 2 punktą). Toks apibrėžimas apima tokias sąvokas kaip *duomenų saugumas*, *tinklų ir informacinių sistemų atsparumas* bet kokiai grėsmei ir kartu indikuoja apie informacinių sistemų, kaip informacinių technologijų priemonių pagalba sukurto informacijos apdorojimo įrankio, paskirtį – paslaugų teikimą informacinės sistemos naudotojams (vidiniams ir išoriniams), informacinės sistemos paslaugų gavėjams. Pagal TIS 2 direktyvos 21 straipsnio 2 dalį tinklų ir informacinių sistemų saugumas turi apimti bent šių minimalių kibernetinio

saugumo elementų (veiklų) įgyvendinimą (toliau – minimalūs privalomi kibernetinio saugumo elementai pagal TIS 2 direktyvos 21 straipsnio 2 dalį):

1. rizikos analizę;
2. informacinių sistemų saugumo politiką;
2. incidentų valdymą;
3. veiklos tęstinumą;
4. tiekimo grandinės saugumą;
5. tinklų ir informacinių sistemų įsigijimo, vystymo, priežiūros saugumą;
6. politiką, procedūras, kurios skirtos kibernetinio saugumo rizikos valdymo priemonių veiksmingumui įvertinti;
7. kibernetinės higienos praktiką (pvz., kibernetinio saugumo mokymus);
8. kriptografinių priemonių naudojimą ir šių priemonių naudojimo politiką, procedūras;
10. žmogiškųjų išteklių saugumą,
11. prieigos kontrolės valdymą, įskaitant prieigos politiką ir procedūras;
12. turto valdymą;
11. saugių sprendimų (pvz. kelių veiksnių tapatumo, saugių ryšių) ir sistemų naudojimą.

Siekiant sisteminio požiūrio į visus minimalius privalomus kibernetinio saugumo elementus bus atsižvelgiama kuriant objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelį.

Verta pažymėti, kad Lietuvos nacionalinė teisė pasižymi skirtingų sąvokų, skirtų informacinių sistemų ir tinklų saugumui apibūdinti, gausa. Štai tik keletas jų: *informacinių sistemų saugumas, informacinių išteklių sauga (LRĮ XI-1807, 2011), ryšių ir informacinių sistemų saugumas (LRĮ, XII-1428, 2014), informacijos ryšių ir informacinė sistemos apsauga (LRĮ VIII-1443, 1999)*. Tokią sąvokų gausą sąlygoja tai, kad Lietuvos Respublikoje „nėra konsoliduotas kibernetinio saugumo ir elektroninės informacijos saugos teisinis reguliavimas“ (Valstybinio audito ataskaitos 17 psl.). Kadangi šiame darbe yra nagrinėjamas informacinės sistemos kibernetinis saugumas, prioritetas bus teikiamas TIS 2 direktyvoje ir Lietuvos Respublikos kibernetinio saugumo įstatyme nustatytoms sąvokoms, nes Lietuvos Respublikos kibernetinio saugumo įstatyme vartojama sąvoka ryšių ir informacinė sistema (toliau – RIS) labiausiai atitinka TIS 2 direktyvoje nustatytą tinklų ir informacinių sistemų sąvoką. RIS saugumas apima elektroninių ryšių tinklus, informacines sistemas, registrus, pramoninių procesų valdymo sistemas, šių sistemų valdymo, naudojimo, apsaugos ir priežiūros tikslais laikomą, tvarkomą, atkuriamą arba perduodamą elektroninę informaciją ir jos saugumo užtikrinimą.

Kibernetinio saugumo sąvoka Lietuvos nacionalinėje teisėje yra labai komplikuota ir plati. Kompleksiškai vertinant RIS ir kibernetinio saugumo sąvokų turinį, darytina išvada, kad RIS kibernetinis saugumas – tai visuma teisinių, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti RIS atsparumą įvairiems kibernetinėje erdvėje esantiems veiksniams, kurie kelia grėsmę RIS,

joje tvarkomos ir (ar) RIS pagalba perduodamos elektroninės informacijos prieinamumui, vientisumui ir konfidencialumui, RIS veikimui, RIS valdymui arba RIS pagalba teikiamoms paslaugoms, taip pat kuriomis siekiama atkurti įprastinę RIS veiklą. Toks RIS kibernetinio saugumo apibrėžimas yra ilgas, bet detalus, jis nurodo kokia apimtimi turėtų būti vertinamas RIS kibernetinis saugumas.

Apibendrinant mokslinėje literatūroje ir teisiniuose šaltiniuose įtvirtintas sąvokas, galima teigti, kad informacinės sistemos kibernetinis saugumas – tai informacinės sistemos gebėjimas būti atspariai bet kokiam informacijos saugumo įvykiui, bet kokiai grėsmei, kuri gali kilti kibernetinėje erdvėje ir informacinės sistemos veikimo ribose. Plačiąja prasme informacinės sistemos kibernetinis saugumas yra susijęs su elektroninės informacijos saugumo (konfidencialumo, vientisumo ir prieinamumo) užtikrinimu kibernetinėje erdvėje viso informacinės sistemos gyvavimo ciklo metu (žr. 1 pav.).

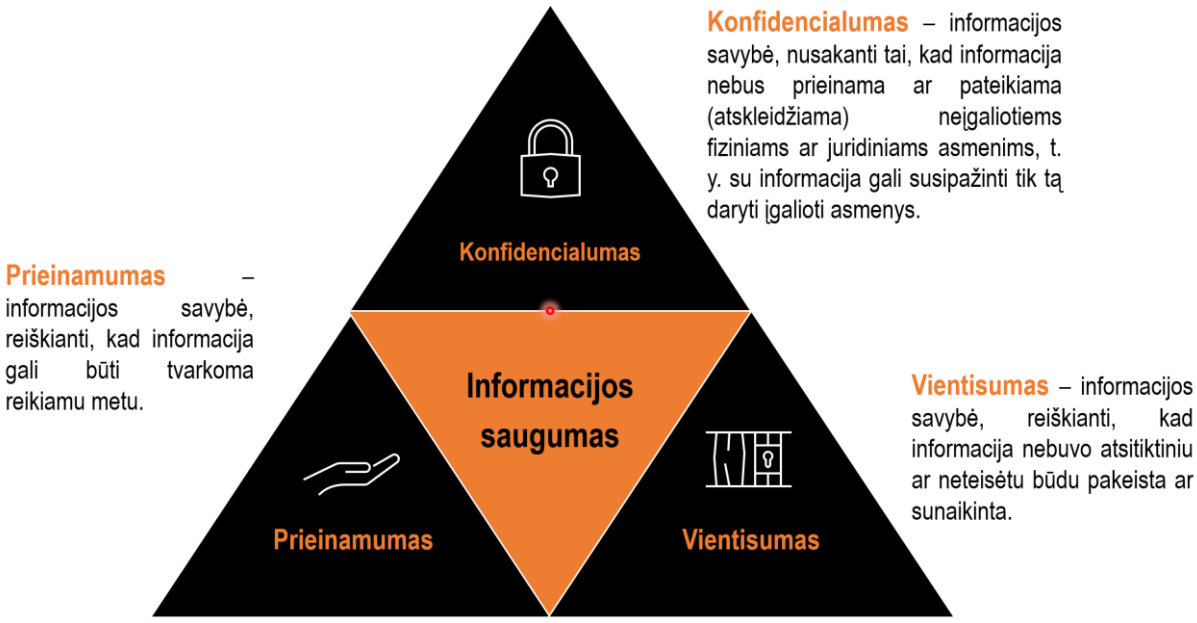
Lietuvos nacionalinės teisės požiūriu RIS kibernetinis saugumas visų pirma yra tiesiogiai susijęs su kibernetine erdve ir jis turi apimti bent šiuos pagrindinius informacinės sistemos kibernetinio saugumo valdymo elementus (toliau – minimalūs RIS kibernetinio saugumo valdymo elementai):

1. elektroninės informacijos ir duomenų saugumo valdymą;
2. techninės ir programinės įrangos saugumo valdymą;
3. ryšių, tinklų saugumo valdymą;
4. teisinių ir organizacinių priemonių valdymą;
5. paslaugų (įskaitant teikiamų trečiųjų asmenų, pvz. paslaugų teikėjų) valdymą;
6. personalo valdymą;
7. rizikų valdymą;
8. veiklos atkūrimo valdymą (pvz. įvykus elektroninės informacijos saugos incidentui);
9. aplinkos saugumo valdymą.

Siekiant visuminio požiūrio šiame darbe į visus Lietuvos nacionalinėje teisėje nustatytus minimalius RIS kibernetinio saugumo valdymo elementus bus atsižvelgiama kuriant objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelį.

1.2. Informacinės sistemos kibernetinio saugumo vertinimo proceso apimtis.

Informacinių sistemų kibernetinio saugumo vertinimas grindžiamas moksline informacijos saugumo užtikrinimo teorija. Ji remiasi pagrindiniais informacijos saugumo užtikrinimo tikslais, kuriuos dar 1981 m. apibrėžė Donn B. Parker savo saugumo modelyje, kuris žinomas kaip triada (angl. *confidentiality integrity availability*, CIA modelis, žr. 2 pav.) (Parker D. B., 1981). Informacinės sistemos kibernetinio saugumo užtikrinimo tikslas – apsaugoti informacinę sistemą, joje saugomą, tvarkomą, informaciją nuo grėsmių, t.y. užtikrinti, kad nebus pažeistas informacijos saugumas (konfidencialumas, vientisumas ir prieinamumas).



2 pav. Informacijos saugumo tikslų triada (CIA modelis)

Šaltinis: parengta šio darbo autorės

Informacinių sistemų konfidencialumo, vientisumo ir prieinamumo užtikrinimo procesas paremtas viena pagrindinių informacijos saugumo koncepcijų – rizikos valdymu. Yra daug metodų, kuriais vadovaujantis galima atlikti informacinių sistemų rizikos vertinimus (pvz. ISO/IEC 27005, NIST SP800-30 ir kt.). Kibernetinė rizika visais atvejais yra tiesiogiai susijusi su informacinėmis technologijomis, informacijos apdorojimo priemonėmis (Jevsejev R., 2019). Mokslinėje literatūroje išskiriami tokie pagrindiniai informacinės sistemos rizikos valdymo proceso komponentai:

1. grėsmių vertinimas,
2. pažeidžiamumų vertinimas, įskaitant saugumo testavimus,
3. saugumo lygio vertinimas.

Grėsmių vertinimas paprastai apima galimų grėsmių informacinei sistemai nustatymą ir jų pasireiškimo tikimybės bei poveikio įvertinimą. Pagal Vostrecovą E.B, informacijos saugumo užtikrinimo triados pagrindu vertinant informacinių sistemų saugumui kylančias grėsmes, galima išskirti tokias 3 pagrindines informacinėms sistemoms kylančias grėsmes (Вострецова Е.В., 2019):

1. Grėsmė informacinės sistemos konfidencialumui (realizuojama kai gaunama nesankcionuota prieiga (tyčia arba atsitiktinai) prie informacijos, saugomos informacinėje sistemoje arba perduodant informaciją iš vienos informacinės sistemos į kitą);

2. Grėsmė informacinės sistemos vientisumui (realizuojama kai nesankcionuotai (tyčia arba atsitiktinai) yra keičiama informacija, saugoma informacinėje sistemoje, arba perduodama iš vienos informacinės sistemos į kitą);

3. Grėsmė informacinės sistemos prieinamumui (realizuojama kaip paslaugų atkirtimas (tyčinis arba atsitiktinis), kurio metu prarandama prieiga prie informacinės sistemos, joje saugomos, jos pagalba tvarkomos informacijos).

Pažeidžiamumų vertinimas, saugumo testavimai, padeda organizacijoms objektyviai įvertinti informacinių sistemų saugumo lygį, gebėjimą apsisaugoti nuo informacinei sistemai kylančių grėsmių. Kai kurie mokslininkai (Fathi S., Hikal N., 2019) moksliniuose tyrimuose informacinių sistemų pažeidžiamumo vertinimus, įsilaužimų vertinimus (angl. *penetration testing*) laiko vieninteliu efektyviausiu kibernetinio saugumo vertinimo metodu.

Informacinės sistemos saugumo lygis vertinamas atsižvelgiant į informacijos, kuri apdorojama informacinėje sistemoje, lygį, vertinant priemones, taikomas atitinkamiems informacinės sistemos informacijos saugumo lygiams užtikrinti.

Tarptautinė geroji praktika, Europos Sąjungos, Lietuvos nacionaliniai teisės aktai rekomenduoja informacinių sistemų kibernetinio saugumo rizikos vertinimus atlikti vadovaujantis tarptautiniais standartais ir metodais (pvz. ISO/IEC, NIST standartais), pagrįstais rizikos valdymu, integruoti informacinių sistemų rizikos vertinimo procesą į organizacijos veiklos rizikos vertinimo procesus. Daugelis mokslininkų pabrėžia, kad gerosios praktikos metodai grindžiami CIA modeliu, tarptautine patirtimi, žiniomis ir pateikia tiek reikalavimus, tiek praktines rekomendacijas kaip organizacijoms pasiekti atitikties nustatytiems kibernetinio saugumo reikalavimams (Kandsamy K, Srinivas S., 2020).

Vienas svarbiausių informacinės sistemos saugumo užtikrinimo komponentų – pagrįstas ir proporcingas informacijos saugumo valdymo ir kontrolės priemonių naudojimas. Tokių priemonių diegimas organizacijai leidžia suplanuoti (numatyti) informacinės sistemos vertinimo metu nustatytų rizikų mažinimo priemones (atsakomąsias priemonės). Lietuvos nacionalinėje teisėje informacinių sistemų kibernetinio saugumo valdymo priemonės skirstomos į dvi kategorijas: organizacines priemones ir technines priemones. Mokslinėje literatūroje egzistuoja ir kitokių informacijos saugumo valdymui skirtų priemonių klasifikavimo kriterijų, pvz. skirstymas pagal CIA modelį į:

1. priemones informacijos konfidencialumui užtikrinti,
2. priemones informacijos vientisumui užtikrinti,
3. priemones informacijos prieinamumui užtikrinti.

Šiame darbe, siekiant visuminio požiūrio, kuriant objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelį, informacinių sistemų kibernetinio saugumo valdymui skirtos priemones, vadovaujantis gerosios praktikos metodais (pvz. ISO/IEC 27001), skirstomos į tokias tris kategorijas:

1. Organizacinės priemonės;
2. Techninės priemonės;
3. Fizinės priemonės.

Organizacinės priemonės apima tokias informacinės sistemos saugumui užtikrinti nustatytas ir taikomas valdymo priemones, kaip:

1. Reikalavimus informacinės sistemos ir joje tvarkomos informacijos kibernetiniam saugumui užtikrinti, kurie paprastai išdėstomi informacinės sistemos saugumo politikos dokumentuose (pvz., organizacijos informacijos saugumo valdymo politikoje, informacinės sistemos saugos nuostatuose) arba kituose organizacijos informacijos saugumo užtikrinimui skirtuose dokumentuose, gairėse.

2. Reikalavimų įgyvendinimo procedūras (veiklos valdymo procesus), kurie paprastai išdėstomi organizacijos informacijos valdymo ir (arba) informacinės sistemos saugumo politiką įgyvendinančiuose dokumentuose (pvz., organizacijos informacijos saugumo valdymo sistemos dokumentuose, procesuose, informacinės sistemos naudotojų valdymo taisyklėse, elektroninės informacijos valdymo taisyklėse ir pan.).

3. Personalo veiklos valdymą, kuris turėtų apimti bent tokių priemonių įgyvendinimą kaip: įgaliojimų personalui suteikimą, funkcijų atskyrimą, personalo mokymus, kibernetinio saugumo kompetencijų ugdymą, trečiųjų šalių teikiamų paslaugų kontrolę ir pan. Personalo sąmoningumo ir atsparumo kibernetinėms grėsmėms brandumo lygiui nustatyti (įvertinti) rekomenduojama periodiškai taikyti socialinės inžinerijos pažeidžiamumų testavimus (angl. *Social Engineering Penetration Test*).

Techninės kontrolės priemonės apima informacinės sistemos saugumui užtikrinti naudojamų techninių ir programinių priemonių (pvz., ugniasienių, įsibrovimų aptikimo sistemų, duomenų šifravimui skirtų sprendimų, privilegijuotos prieigos valdymo sistemos ir pan.) parinkimą, naudojimą, atsižvelgiant į organizacijos veiklos pobūdį, tvarkomos informacijos kategoriją (lygį), jų administravimą, priežiūrą, atnaujinimą viso šių priemonių gyvavimo ciklo metu. Šių priemonių saugumo lygiui, atitikties kibernetinio saugumo reikalavimams ir gebėjimų apsisaugoti nuo informacinei sistemai kylančių grėsmių vertinimui atlikti rekomenduojama periodiškai taikyti technologinio pažeidžiamumo patikrinimo testavimus (angl. *penetration testing*).

Fizinės kontrolės priemonės apima informacinės sistemos fizinės aplinkos saugumui skirtas valdymo priemones. Jos gali būti tiek techninės – programinės (pvz. vaizdo stebėjimo sistema, įeigos kontrolės sistema (mechaninė ir (arba) elektroninė), priešgaisrinės apsaugos, apsaugos nuo įsibrovimų sistema ir pan.) tiek organizacinės (pvz. žmogiškojo faktoriaus pagrįsti apsaugos sprendimai). Informacinės sistemos fizinės aplinkos saugumo lygį ir atsparumą grėsmėms galima patikrinti socialinės inžinerijos metodu, t.y. atliekant socialinės inžinerijos pažeidžiamumų testavimus (angl. *Social Engineering Penetration Test*).

Pastaraisiais metais daugelis mokslininkų (Shouran Z., Priambodo T., 2019, Grinevičius R., 2019, Asfoor A., Kasim H., 2022) tyrimuose vis dažniau akcentuoja žmogaus, kaip efektyvios organizacijos informacinės ekosistemos saugumo priemonės svarbą ir žmogaus įtaka užtikrinant organizacijos valdomos informacijos, informacinių sistemų kibernetinį saugumą. Gartner įmonė,

teikdama rekomendacijas įmonių vadovams (Gartner, 2022) pažymi, kad progresyvios organizacijos turi peržengti darbuotojų informavimo apie saugumo reikalavimus ribas, jos privalo investuoti į personalo holistinio elgesio ir kultūros programas, skirtas saugesniems darbo su informacija būdams skatinti – tai šiuolaikinė kibernetinio saugumo tendencija. Pažymėtina, kad ENISA dar 2018 m. parengė rekomendacijas organizacijoms, kuriose akcentuojama žmogiškųjų išteklių valdymo programų kūrimo svarba. Žmogiškuosius kibernetinio saugumo aspektus ENISA siūlo vertinti kaip nuolatinį organizacijos kibernetinio sąmoningumo ugdymo procesą. Šiame darbe į šią saugumo priemonę taip pat bus atsižvelgiama kuriant objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelį.

Atliekant informacinės sistemos kibernetinio saugumo vertinimą labai svarbu nustatyti vertinamos informacinės sistemos veiklos (funkcionavimo) aplinką. Skirtingose aplinkose nustatomi skirtingi informacinės sistemos veiklos režimai, taikomos skirtingos organizacinės, techninės ir fizinės priemonės. „Organizacijos informacinė sistema kartu yra ir žmonių darbo įgūdžių, informacijos, informacinių technologijų ir veiklos procesų derinys“ (Dzemydienė D., Naujikienė R, 2004). „Be to, galima išskirti kitokią ribą sistemoje, skiriančią rankinius darbus nuo kompiuterizuotų darbų. Ši riba vadinama automatizuotų darbų riba“ (Barčkutė O., 2008). Šiame darbe, kuriant objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelį, į šį kriterijų taip pat bus atsižvelgiama.

Informacinių sistemų kibernetinio saugumo vertinimo procesas apima įvairias mokslo disciplinas – kompiuterių mokslą, inžineriją, vadybą ir teisę. Iš informacinių sistemų kibernetinio saugumo vertinimą organizuojančių, vertinimo procese dalyvaujančių specialistų reikalaujama skirtingų žinių ir kompetencijų. ENISA 2022 m. rugsėjo mėn. atnaujino Europos kibernetinio saugumo kompetencijų sąrašą (angl. *European Cybersecurity Skills Framework,* ECSF), kuriame išskyrė 12 kibernetinio saugumo specialistų roles (žr. 1 lentelę). Tačiau Lietuvos mokslininkų atliktais moksliniais tyrimais įrodyta, kad toks ENISA ECSF kompetencijų sąrašas Lietuvoje yra netaikomas. Lietuvoje iš kibernetinio saugumo specialisto reikalaujama atlikti kelių rolių veiklas organizacijoje, dažniausia ne mažiau kaip trijų, šio darbo 1 lentelėje nurodytų, kibernetinio saugumo specialistų rolių. Pažymėtina, kad Lietuvos įmonėse ir organizacijose, nepriklausomai nuo jų dydžio, dažnai už kibernetinio saugumo įgyvendinimą atsakingu paskiriamas technologinių žinių specialistas (Bukauskas L., Brilingaitė A., 2022), net tuo atveju kai organizacijoje yra atskiriamos techninės ir netechninės kibernetinio saugumo specialistų rolės iš netechninių kompetencijų specialistų, pavyzdžiui informacijos saugos vadovų (angl. *chief information security officer, CISO*), dažnai reikalaujama atlikti techninių kompetencijų rolių specialistų funkcijas (Bukauskas L., Brilingaitė A., 2022). Toks ydingas požiūris į specialistų, atsakingų už informacinių sistemų kibernetinį saugumą, jų vykdomas roles ir atsakomybes, parodo pakankamai žemą kibernetinio saugumo srities brandos lygį Lietuvoje ir poreikį keisti susiklosčiusią ydingą praktiką.

1 lentelė ENISA kibernetinio saugumo specialistų rolių sąrašas

Nr.	Rolės pavadinimas anglų kalba	Rolės vertimas
1.	Chief information security officer (CISO)	Vyr. informacijos saugos vadovas
2.	Cyber incident responder	Reagavimo į incidentus ekspertas
3.	Cyber legal, policy and compliance officer	Kibernetinės teises, politikos ir atitikties pareigūnas
4.	Cyber threat intelligence specialist	Kibernetinių grėsmių, žvalgybos pareigūnas
5.	Cybersecurity architect	Kibernetinio saugumo architektas
6.	Cybersecurity auditor	Kibernetinio saugumo auditorius
7	Cybersecurity educator	Kibernetinio saugumo sąmoningumo ugdytojas
8	Cybersecurity implementer	Kibernetinio saugumo įgyvendintojas (inžinierius)
9	Cybersecurity researcher	Kibernetinio saugumo tyrimų ekspertas (inžinierius)
10	Cybersecurity risk manager	Kibernetinio saugumo rizikos vadovas (analitikas)
11	Digital digital forensics investigator	Skaitmeninių nusikaltimu tyrėjas (analitikas)
12	Penetration tester	Pažeidžiamumu testuotojas, etiškas įsilaužėlis

Šaltinis: parengta šio darbo autorės pagal ENISA European Cybersecurity Skills Framework Role Profiles, prieiga per internetą: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

Atsižvelgiant į tai, kad informacinės sistemos kibernetinio saugumo vertinimo procesas turi būti periodinis ir sistemingas, pagrįstas visuotinai pripažintomis informacijos saugumo valdymo strategijomis (pvz. tarptautiniais standartais), informacinės sistemos kibernetinio saugumo vertinimo procesui įgyvendinti būtina numatyti kokias standartizuotas informacijos, informacinių technologijų saugumo užtikrinimui skirtas strategijas ir metodus taikyti. Pasinaudojus viena arba keliomis, struktūrizuotomis, gerai apibrėžtomis informacinių sistemų/informacijos saugumui įvertinti skirtomis strategijomis, metodais arba jų deriniu, galima ne tik objektyviai įvertinti informacinės sistemos kibernetinio saugumo būklę, bet ir numatyti: rizikų mažinimo priemones, įgyvendinti pažangos stebėseną, organizacijos veiklos efektyvumui skirtas priemones bei veiklas, skirtas tobulinti organizacijos informacinės sistemos apsaugos sistemą, informacijos saugumo valdymo sistemą (toliau – ISVS).

Siekiant objektyvaus ir gerąja praktika paremto vertinimo, informacinių sistemų kibernetinio saugumo vertinimo specialistui būtina žinoti visuotinai pripažintus saugumo standartus, rekomendacijas ir metodus, ypač kai standartų reikalavimų laikymąsi numato nacionalinė teisė. Tarptautinių ir nacionalinių standartų informacijos, informacinių sistemų saugumo valdymo, rizikų valdymo srityje yra daug. Atsižvelgiant į tai, kad šiame darbe kuriamas informacinės sistemos vertinimo kibernetinio saugumo aspektu modelis bus tikrinamas atliekant empirinį tyrimą Lietuvos Respublikoje registruotų valstybės informacinių sistemų valdytojų ir (ar) tvarkytojų valdomų informacinių sistemų atžvilgiu tikslinga apžvelgti Lietuvos nacionalinėje teisėje nustatytus, valstybės informacinių sistemų valdytojams ir (ar) tvarkytojams rekomenduojamus taikyti, atitikties kibernetinio saugumo reikalavimams metodus bei svarbiausius tarptautinius standartus, kuriuose užfiksuoti kvalifikuotų specialistų sukurti kokybiški sprendimai ir metodai tokiam vertinimui atlikti.

Apibendrinant tai, kas išdėstyta, galima teigti, kad siekiant visapusiško ir objektyvaus informacinės sistemos kibernetinio saugumo vertinimo, informacinės sistemos vertinimo procese turi

dalyvauti skirtingų žinių ir kompetencijų specialistai, vertinimo procesas turi būti atliekamas vadovaujantis gerąja praktika, taikant gerosios praktikos metodus ir apimti bent šiuos pagrindinius informacinės sistemos kibernetinio saugumo vertinimo elementus:

1. Rizikų vertinimą;
2. Informacinės sistemos saugumui užtikrinti taikomų valdymo priemonių (teisinių, organizacinių, techninių, fizinių) vertinimą;
3. Informacinės sistemos veiklos (funkcionavimo) aplinkos vertinimą;
4. Informacinės sistemos technologinio pažeidžiamumo patikrinimą (angl. *penetration testing*);
5. Socialinės inžinerijos pažeidžiamumų testavimus (angl. *Social Engineering Penetration Test*).

Siekiant visuminio požiūrio į visus išvardintus informacinės sistemos kibernetinio saugumo vertinimo elementus bus atsižvelgiama kuriant objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelį.

1.3. Informacinės sistemos kibernetinio saugumo vertinimui taikomi moksliniai gerosios praktikos metodai

Dauguma organizacijų, siekdamos užtikrinti informacinių sistemų saugumą, taiko įvairias informacijos saugumo valdymo priemones. Tačiau, nesant aiškios, struktūrizuotos valdymo sistemos, tokios priemonės įgyvendinamos kaip atsakas konkrečiai situacijai, t.y. *ad hoc* principu. Veiksmingas kibernetinio saugumo, elektroninės informacijos saugumo užtikrinimas priklauso nuo tinkamų ir proporcingų, informacijos saugumo principų nustatymo, saugumo metodų taikymo ir informacijos saugumo valdymo procesų organizavimo. Tarptautinės organizacijos, tarptautinės asociacijos (pvz., ISO, NIST, ISACA, SANS ir kt.) buvo įsteigtos tam, kad nustatytų standartizuotus reikalavimus, taisykles ir (ar) procedūras, kurias rekomenduotina taikyti tiek projektuojant saugią informacinių technologijų infrastruktūrą, tiek užtikrinant minimalų tokios infrastruktūros saugumą. Informacinių sistemų vertinimo procesą organizuojantiems specialistams standartai yra instrumentas, leidžiantis nustatyti, ar informacinė sistema, informacinis technologijų produktas, informacijos valdymo politika atitinka saugumo reikalavimus. Todėl verta išnagrinėti pagrindinius, pasaulinėje praktikoje taikomus, informacinių sistemų ir informacijos saugumo valdymui ir vertinimui skirtus standartus, metodus.

1.3.1. ISO 27001 standarto metodas

ISO/IEC 27001 yra pagrindinis tarptautinis standartas, apibrėžiantis ISVS reikalavimus. Geroji informacijos, informacinių technologijų valdymo praktika rekomenduoja organizacijoms sukurti ISVS, kuri reglamentuotų organizacijos saugumo principus, formalius ir nuolatinius informacijos, informacinių technologijų saugumo valdymo metodus, užtikrintų organizacijoje nustatytos saugumo

politikos, principų, standartų, procedūrų, metodikų atitiktį visiems taikomiems tarptautiniams reikalavimams. ISVS kūrimo, veikimo ir plėtros reikalavimus, kontrolės priemonių tikslus ir kontrolės priemones nustato ISO/IEC 27001 standartas. Atskiroms sritims ir sektoriams taikytinus saugumo reikalavimus nustato kiti ISO 27000 šeimos standartai ir vadovai. Diegiant ISVS kartu su ISO/IEC 27001 standartu taikomas ISO/IEC 27002 standartas, kurį galima vadinti ISVS praktikos kodeksu. Reikalavimai, nustatyti ISO/IEC 27001 įgyvendinami taikant ISO/IEC 27002 standarte nustatytas informacijos saugumo kontrolės priemones.

ISVS užtikrina informacijos saugumo (konfidencialumo, vientisumo ir prieinamumo) valdymą, taikant rizikos valdymo procesą. ISVS padeda organizacijai susisteminti informacijos saugumo valdymo procesus, nustatyti aiškias valdymo priemones, susieti informacinių technologijų ir informacijos saugumo procesus su organizacijos veiklos procesais. ISVS įdiegimas organizacijoje leidžia užtikrinti organizacijos klientus, kad rizikos, susijusios su informacijos saugumu yra tinkamai valdomos. Tarptautinėje praktikoje daroma prielaida, kad organizacija, įdiegusi ISVS, taiko visas informacijos saugumo valdymo ir kontrolės priemones, nustatytas ISO/IEC 27001 standarte. ISVS tikslas – pasiekti priimtiną organizacijai rizikos lygį, apsaugoti informaciją, informacinę infrastruktūrą, informacines sistemas ir kitus informacinius išteklius nuo galimo tyčinio ir atsitiktinio poveikio.

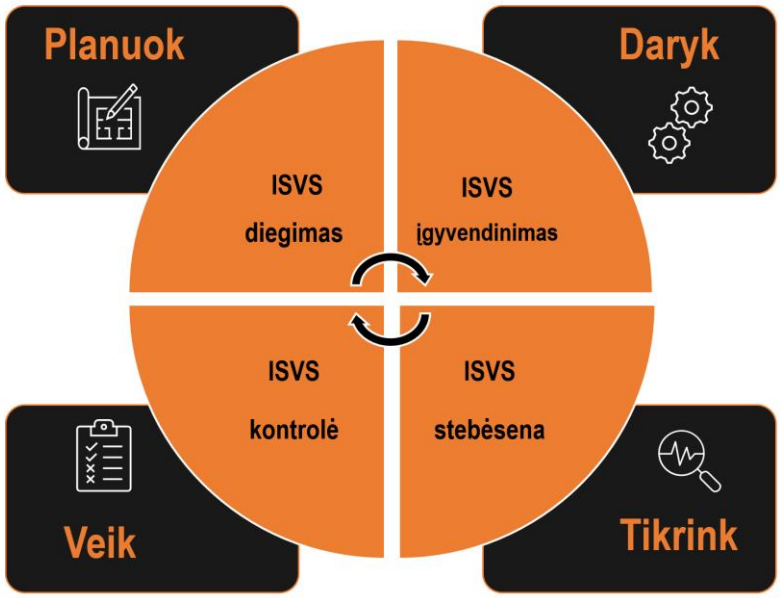
ISO/IEC 27001 standartą sudaro tokie skyriai (toliau – ISVS privalomi minimalūs informacijos saugumo valdymo elementai):

1. Informacijos saugumo politika (A.5)
2. Informacijos saugumo organizavimas (A.6)
3. Žmogiškųjų išteklių saugumas (A.7)
4. Turto valdymas (A.8)
5. Prieigos valdymas (A.9)
6. Kriptografija (A.10)
7. Fizinis ir aplinkos saugumas (A.11)
8. Darbo saugumas (A.12)
9. Ryšių saugumas (A.13)
10. Sistemų įsigijimas, kūrimas ir priežiūra (A.14)
11. Santykiai su tiekėjais (A.15)
12. Informacijos saugumo incidentų valdymas (A.16)
13. Veiklos tęstinumo valdymo informacijos saugumo aspektai (A.17)
14. Atitiktis (A.18)

Kiekviename skyriuje yra sąsajos su kito skyriaus procesu ar jų kombinacija.

ISO/IEC 27001 standartas sudarytas „procesinio požiūrio“ principu, kurio privalumas – nenutrūkstantis procesų, jų kombinacijų ir sąveikos valdymas ir tobulinimas. Viena iš procesinio

valdymo diegimo metodikų – klasikinis uždaras informacijos saugumo valdymo ir tobulinimo ciklas dar žinomas kaip „Demingo ciklas“ arba planuok – daryk – tikrink – veik metodas (angl. *Plan–Do–Check–Act, PDCA*) (žr. 3 pav.).



3 pav. Informacijos saugumo valdymo ir tobulinimo ciklas (PDCA metodas)
Šaltinis: parengta šio darbo autorės

PDCA metodas gali padėti organizacijai nustatyti veiklos kontekstą (sritį), apibrėžti standarto taikymo apimtį ir tikslus. Tiek ISO/IEC 27001 standartas tiek PDCA metodas pagrįsti rizikos vertinimu, neatitikčių valdymu, kontrolės priemonių parinkimu, turimų kontrolės priemonių įgyvendinimu. Kai kurie mokslininkai (Kandsamy K., Srinivas S., 2020, Palko D., Babenko T., 2023) pabrėžia ISO/IEC 27001 standarto svarbą rizikos vertinimo procese, nes jis nustato informacijos saugumo rizikos vertinimo kriterijus, leidžia parinkti organizacinius mechanizmus informacinės sistemos rizikoms mažinti. Kiti mokslininkai (Junaid T. S., 2023) akcentuoja šio standarto didžiulę ekonominę ir reputacinę naudą, nes ISVS diegimas ne tik sumažina informacijos saugumo atakų daromą ekonominę ir reputacinę žalą, bet ir įtikina organizacijos klientus, partnerius, kad įvykus saugumo incidentui bus imtasi visų būtinų veiksmų siekiant išsaugoti organizacijos informaciją (turtą) atakos atveju.

ISO/IEC 27001 standartas, kaip informacijos saugumo vertinimo metodas, yra tinkamas organizacijoms, kurios siekia žingsnis po žingsnio įdiegti veiksmingą ISVS, užtikrinti informacijos saugumo valdymo kontrolę, sumažinti rizikas, siekti nuoseklaus veiklos tobulinimo ir informacijos saugumo procesų integravimo į organizacijos veiklos procesus. Standartas reikalauja periodiškai atlikti vidinius ir išorinius ISVS atitikties vertinimus, auditus. Tokiu būdu yra tenkinamas nuolatinis organizacijos poreikis mažinti su informacijos saugumu susijusias rizikas ir poreikis tobulinti veiklos

procesus. Organizacijoms, atitinkančioms ISO/IEC 27001 reikalavimus ir atlikusioms sertifikavimo procesą yra suteikiamas atitikties šiam standartui sertifikatas, kuris įrodo, kad organizacijoje naudojamos visos būtinos priemonės informacijos konfidencialumui, vientisumui ir prieinamumui apsaugoti. 2022 m. spalio 28 d. buvo išleista naujausia ISO 27001 standarto versija, kurioje numatytos naujos informacijos saugumo kontrolės priemonės, pvz. saugus kodavimas (angl. *secure coding*).

Siekiant visuminio požiūrio, šiame darbe visi ISVS privalomi minimalūs informacijos saugumo valdymo elementai bus vertinami kuriant objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelį.

1.3.2. NIST CSF standarto metodas

NIST CSF (angl. *Cyber security framework*) buvo sukurtas siekiant pagerinti kibernetinio saugumo rizikos valdymą kritinėje infrastruktūroje. Kaip ir ISO/IEC 27001 standartas, NIST CSF – tai rizikų valdymu pagrįstas kibernetinio saugumo valdymo metodas, sukurtas taip, kad padėtų organizacijoms supaprastinti veiklos procesus, apibrėžti esamas ir galimas rizikas, nustatyti esamą kibernetinio saugumo lygį, saugumo prioritetus bei tinkamai valdyti biudžetą. Standartas sudarytas iš 3 komponentų, sudarančių standarto karkasą:

1. Branduolio (angl. *Framework Core*),
2. Įgyvendinimo pakopų (angl. *Tiers*),
3. Profilių (angl. *Profiles*).

NIST CSF karkaso branduolyje (angl. *Framework Core*) aprašomos kibernetinio saugumo veiklos, veiksmai, priemonės ir praktikos, skirtos norimam rezultatui, įgyvendinant konkrečias kibernetinio saugumo priemones, pasiekti. Sistemos branduolį sudaro keturi elementai:

1. **Funkcijos** – jų tikslas yra organizuoti pagrindinę organizacijos kibernetinio saugumo valdymo veiklą aukščiausiu lygiu. Funkcijos sudaro organizacijos kibernetinio saugumo rizikos valdymo gyvavimo ciklą, kurį sudaro tokios fazės: identifikuoti, apsaugoti, aptikti, reaguoti, atkurti (angl. *Identify, Protect, Detect, Respond, Recover*). Kiekvienai funkcijai yra priskirtos organizacinių ir techninių priemonių kategorijos (žr. 4 pav.);

2. **Kategorijos** – tai organizacinių ir techninių priemonių grupės, identifikuojančios konkrečias kibernetinio saugumo valdymui skirtas veiklas, pavyzdžiui, „Turto valdymas“ (anglų *Asset Management*) (žr. 4 pav.);

3. **Subkategorijos** – tai kategorijos suskirstymas į konkrečius organizacinių ir techninių priemonių įgyvendinimo rezultatus, pavyzdžiui, identifikuojant verslo aplinką (angl. *Business Environment*, ID.BE) turi būti „Nustatytas organizacijos vaidmuo tiekimo grandinėje (santykiai su tiekėju)“ (žr. 5 pav. ID.BE kategorijos sąsają su ID.BE-1 subkategorija).

4. **Informacinės nuorodos** – tai nuorodų į specifinių standartų, gairių ir praktikų skyrius. Tai pasaulyje paplitusios gerosios praktikos, iliustruojančios metodus, t.y. nurodančios kaip pasiekti su kiekviena subkategorija susietus rezultatus, pavyzdžiui organizacijoms, įdiegusioms ISVS yra naudinga žinoti, kad ID.BE-1 subkategorijai įgyvendinti skirtos praktikos yra aprašytos ISO/IEC 27001 standarto 15.1.1-15.2.2 papunkčiuose (žr. 5 pav.).

FUNKCIJA (Function)	KATEGORIJA (Category)	Funkcijos.Kategorijos identifikacinis Nr. (ID)
Identifikuoti (Identify)	**Turto valdymas** (Asset Management)	ID.AM
	Verslo aplinka (Business Environment)	ID.BE
	Valdymas (Governance)	ID.GV
	Rizikos vertinimas (Risk Assessment)	ID.RA
	Rizikos valdymo strategija (Risk Management Strategy)	ID.RM
	Tiekimo grandinės (Tiekėjų) rizikos valdymas (Supply Chain Risk Management)	ID.SC
Apsaugoti (Protect)	**Tapatybės valdymas ir prieigos kontrolė** (Identity Management and Access Control)	PR.AC
	Sąmoningumas ir mokymai (Awareness and Training)	PR.AT
	Duomenų saugumas (Data Security)	PR.DS
	Informacijos apsaugos procesai ir procedūros (Information Protection Processes and Procedures)	PR.IP
	Priežiūra (Maintenance)	PR.MA
	Apsaugos technologijos (Protective Technology)	PR.PT
Aptikti (Detect)	**Anomalijos ir įvykiai** (Anomalies and Events)	DE.AE
	Saugumo nuolatinė stebėsena (Security Continuous Monitoring)	DE.CM
	Aptikimo procesai (Detection Processes)	DE.DP
Reaguoti (Respond)	**Reagavimo planavimas** (Response Planning)	RS.RP
	Komunikacija (Communications)	RS.CO
	Analizė (Analysis)	RS.AN
	Pasekmių švelninimas (Mitigation)	RS.MI
	Tobulinimas (Improvements)	RS.IM
Atkurti (Recover)	**Veiklos atstatymo planas** (Recovery Planning)	RC.RP
	Pasekmių švelninimas (Improvements)	RC.IM
	Komunikacija (Communications)	RC.CO

4 pav. Rizikos valdymo gyvavimo ciklo funkcijų ir kiekvienai funkcijai priskirtų kategorijų sąrašas

Šaltinis: parengta šio darbo autorės pagal informaciją pateiktą NIST CSF standarte (prieiga per internetą: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf)

Funkcija ,,Identifikuoti" skirta įvertinti išteklius, kurie turi kritinę reikšmę organizacijos veiklai, įvertinti susijusias kibernetinio saugumo rizikas. Šios funkcijos kategorijų pavyzdžiai: Turto valdymas; Verslo aplinka; Valdymas; Rizikos vertinimas; Rizikos valdymo strategija ir Tiekimo grandinės (Tiekėjų) rizikos valdymas (žr. 4 pav.).

Funkcija ,,Apsaugoti" skirta įgyvendinti tinkamas apsaugos priemones. Šios funkcijos kategorijų pavyzdžiai: Tapatybės valdymas ir prieigos kontrolė; Sąmoningumas ir mokymai; Duomenų saugumas Informacijos apsaugos procesai ir procedūros; Priežiūra; Apsaugos technologijos (žr. 4 pav.).

Funkcija ,,Aptikti" skirta laiku aptikti kibernetinio saugumo įvykius. Šios funkcijos kategorijos pavyzdžiai: Anomalijos ir įvykiai; Saugumo nuolatinė stebėsena; Aptikimo procesai (žr. 4 pav.).

Funkcija ,,Reaguoti" – skirta įgyvendinti atitinkamą veiklą, pvz., kad būtų imtasi veiksmų dėl aptikto kibernetinio saugumo incidento. Šios funkcijos kategorijų pavyzdžiai: Reagavimo planavimas; Komunikacija; Analizė; Pasekmių švelninimas; Tobulinimas (žr. 4 pav.).

Funkcija ,,Atkurti“ – skirta įgyvendinti atitinkamą veiklą, kad būtų atkurtos visos paslaugos, kurios buvo sutrikusios dėl kibernetinio saugumo incidento. Šios funkcijos kategorijų pavyzdžiai: Veiklos atstatymo planas; Pasekmių švelninimas; Komunikacija (žr. 4 pav.).

NIST CSF standarte visos kategorijos suskirstomos į konkrečias organizacines ir technines priemones (Subkategorijas). Standartas pateikia nuorodas į specifinius standartus, gaires, praktikas, kuriuos taikant galima pasiekti šių priemonių įgyvendinimo rezultatus (žr. 5 pav.).

FUNKCIJA (Function)	KATEGORIJA (Category)	Nr. (ID)
Identifikuoti (Identify)	**Turto valdymas** (Asset Management)	ID.AM
	Verslo aplinka (Business Environment)	**ID.BE**
	Valdymas (Governance)	ID.GV
	Rizikos vertinimas (Risk Assessment)	ID.RA
	Rizikos valdymo strategija (Risk Management Strategy)	ID.RM
	Tiekimo grandinės (Tiekėjų) rizikos valdymas (Supply Chain Risk Management)	ID.SC

SUBKATEGORIJA (Subcategory)	INFORMACINĖ NUORODA (Informative References)
ID.BE-1: Nustatytas organizacijos vaidmuo tiekimo grandinėje (santykiai su tiekėju)	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC **27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53** Rev. 4 CP-2, SA-12
ID.BE-2: Organizacijos vieta kritinėje infrastruktūroje yra identifikuojama	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53** Rev. 4 PM-8
ID.BE-3: Nustatoma ir skleidžiama informacija apie organizacijos misiją, tikslus ir veiklos prioritetus	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53** Rev. 4 PM-11, SA-14
ID.BE-4: Nustatomos kritinės paslaugos, jų svarbiausios funkcijos	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53** Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Nustatomi atsparumo reikalavimai, skirti palaikyti kritinių paslaugų teikimą	**COBIT 5** BAI03.02, DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53** Rev. 4 CP-2, CP-11, SA-13, SA14

5 pav. Kategorijos ir subkategorijos su informacinėmis nuorodomis sąrašo pavyzdys
Šaltinis: parengta šio darbo autorės pagal informaciją pateiktą NIST CSF standarte (prieiga per internetą: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf)

Organizacijos gali pačios pasirinkti kokiu gerosios praktikos metodu (vieną ar kelis taikant) pasinaudoti, kad būtų pasiektas subkategorijoje aprašytas rezultatas.

NIST CSF karkaso įgyvendinimo pakopos (angl. *Tiers*) skirtos organizacijos brandumo (požiūrio į kibernetinio saugumo riziką) lygiui nustatyti ir atsižvelgiant į nustatytą lygį, pasirinkti atitinkamus procesus kaip riziką valdyti ir kokius brandumo lygius siekti. Organizacijos kibernetinio brandumo lygis (atitiktis vienai iš 4 įgyvendinimo pakopų, kur 1 – tai žemiausias brandos lygis, o 4 – tai aukščiausias brandos lygis) nustatomas vertinant tokius 3 elementus (žr. 6 pav.):

1. Organizacijos rizikos valdymo praktika (procesas);
2. Organizacijos integruota rizikos valdymo programa;
3. Organizacijos išorinis dalyvavimas (santykis su išore).

Organizacijos požiūrio į riziką lygis (angl. Framework Implementation Tier)	Organizacijos rizikos valdymo praktika (procesas) (angl. Risk Management Process)	Organizacijos integruota rizikos valdymo progama (Integrated Risk Management Program)	Organizacijos išorinis dalyvavimas (santykis su išore) (External Participation)
1 lygis - Dalinis (Tier 1 - Partial)	Neformalizuota praktika, valdoma ***ad hoc*** principu (reaktyviu būdu)	Žemas rizikos suvokimo sąmoningumas, nenustatytas rizikos valdymas, nenustatyti valdymo procesai	Organizacija nesuvokia savo vaidmens didesnėje ekosistemoje, su išore (kompetentingomis institucijomis, tiekėjais, kitomis šalimis) nekomunikuojama
2 lygis - Informuotas apie rizikas (Tier 2 – Risk Informed)	Patvirtinta rizikos valdymo praktika, bet netaikoma kaip organizacijos politika (nepatvirtinta vadovybės)	Rizika suvokiama organizacijos lygmeniu, bet nėra susieta su organizacijos veiklos rizikomis, organizacijos tikslais	Organizacija supranta savo vaidmenį didesnėje ekosistemoje, bendradarbiauja su kitais subjektais, gauna informaciją, bet nesidalina ja su kitais subjektais
3 lygis - Būtina kartoti (Tier 3 – Repeatable)	Rizikos valdymo praktika vadovybės patvirtinta kaip politika, reguliariai atnaujinama atsižvelgiant į pokyčius	Sisteminis požiūris, rizikos valdomos, procedūros, procesai nustatyti, integruoti, peržiūrimi, darbuotojai turi būtinų kompetencijų	Organizacija supranta savo vaidmenį didesnėje ekosistemoje ir gali prisidėti prie platesnės bendruomenės rizikos supratimo.
4 lygis - Priimtina / valdoma (Tier 4 – Adaptive)	Nuolat tobulinama rizikos valdymo praktika, remiantis ankstesne, dabartine veikla, išmoktomis pamokomis, aktyviai prisitaikoma prie naujų grėsmių	Rizikos valdomos, procedūros, procesai nustatyti, kibernetinio saugumo rizikos valdymas yra organizacijos kultūros dalis, nuolat mokomasi ir perduodamos žinios (užtikrinamas tęstinumas)	Organizacija supranta savo vaidmenį, prisideda prie platesnės bendruomenės, rizikos supratimo, aktyviai dalinamasi informacija organizacijos viduje ir išorėje

6 pav. Organizacijos brandumo (požiūrio į rizikas) lygio vertinimo pavyzdys

Šaltinis: parengta šio darbo autorės pagal informaciją pateiktą NIST CSF standarte (prieiga per internetą: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf)

NIST CSF siūlomas organizacijos brandumo lygio (požiūrio į rizikas) vertinimo modelis tinka kiekvienai organizacijai, nepriklausomai nuo jos dydžio ir neatsižvelgiant į jos valdomų ir (ar) tvarkomų informacinių sistemų sudėtingumą.

NIST CSF karkaso profiliai (angl. *Profiles*) skirti organizacijoms sukurti tinkamą kibernetinio saugumo rizikos mažinimo planą, suderintą su organizacijos tikslais, atsižvelgiant į organizacijos brandos lygį ir įvertinus teisinius/reguliacinius reikalavimus, taikant geriausią praktiką, nustatyti rizikos valdymo prioritetus.

Laikomasi nuomonės, kad organizacijos, naudojančios NIST CSF metodą, turi gebėti išmatuoti ir įvertinti rizikos vertes, atlikti veiksmų sąnaudų ir naudos vertinimą, sumažinti riziką iki priimtino lygio. Kuo geriau organizacija įvertina rizikas, kuo objektyviau nustato savo brandumo lygį, tuo geriau, racionaliau ir efektyviau ji taikys (parinks) kibernetinio saugumo priemones ir valdys joms skirtas investicijas. Kai kurie mokslininkai (Kandsamy K, Srinivas S., 2020) pabrėžia NIST CSF standarto svarbą informacinės sistemos rizikos vertinimo procese, nes NIST CSF nustato mažiausiai tris rizikos valdymo tikslus: įrangos saugumo užtikrinimą, informacijos (duomenų) saugumo užtikrinimą, veiklos atkūrimo (tęstinumo) užtikrinimą.

Siekiant visuminio požiūrio, šiame darbe į visas NIST CSF organizacinių ir techninių priemonių kategorijas (žr. 4 pav. antrą stulpelį) bus atsižvelgiama kuriant objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelį.

1.3.3. CIS Controls standarto metodas

Visame pasaulyje pripažintas informacinių technologijų sistemų ir duomenų apsaugos metodas CIS Controls (angl. *Critical Security Controls, CSC*) apima kritines saugumo kontrolės priemones ir yra rekomenduojamas organizacijai, siekiančiai užtikrinti efektyvią kibernetinio saugumo gynybą. CIS Controls – tai kibernetinės gynybos veiksmų rinkinys, suteikiantis konkrečius ir veiksmingus būdus kaip sustabdyti labiausiai paplitusias ir pavojingiausias atakas. 2021 m. gegužės 18 d. CIS pristatė 8 versiją CIS Controls metodo, kurioje kontrolės priemonės atnaujintos atsižvelgiant į šių dienų aktualijas, kai informacinės infrastruktūros palaipsniui visiškai pereina į debesijos paslaugų aplinką.

CIS Controls modelis kuria prioritetais, grėsmėmis ir rizika paremtą požiūrį į saugumą. Pagrindinis dėmesys kreipiamas į automatizaciją. Siekiant finansinio efektyvumo, apčiuopiamų rezultatų, patikimumo ir plėtimosi galimybių efektyvi kibernetinės erdvės gynyba turėtų remtis tokiais principais:

1. ,,Puolimas informuoja gynybą“, kuris reiškia, kad žinios apie tikras atakas turi būti panaudojamos siekiant sukurti efektyvią gynybą;
2. Prioretizavimas, kuris reiškia, kad pirmiausia reikėtų investuoti į priemones, kurios labiausiai gali sumažinti rizikas, pasiūlyti apsaugą nuo pavojingiausių grėsmių, nesudėtingai pritaikomus organizacijos informacinėje infrastruktūroje, veikloje (pvz. investuoti į ,,greituosius laimėjimus“).
3. Metrikų kūrimu, kuris reiškia bendrų matavimo kriterijų, kurie padeda susikalbėti organizacijos vadovams, techniniam personalui, auditoriams ir saugumo specialistams, numatymas;
4. Pastovios stebėsenos – tai nenutrūkstantis saugumo būklės stebėjimas ir auditavimas.
5. Automatizacija – tai gynyba, pagrįsta automatizuotais sprendimais.

Aštuntos versijos CIS Controls modelį sudaro 18 kibernetinei gynybai skirtų saugumo kontrolės priemonių, kurios siūlo 153 saugumo priemones, suskirstytas į 3 įgyvendinimo lygius (žr. 7 pav.).

CIS Controls modelis numato 7 ,,greitus laimėjimus“, t.y. išskiria saugumo priemones, kurios yra prioritetinės dėl savo efektyvumo stabdant daugumą kryptingų, didžiausią žalą darančių, įsibrovimų (Huges C., 2021):

1. Sudaryti leistinos techninės ir programinės įrangos sąrašus (žr. 7 pav. valdymo priemones Nr. 01 ir Nr. 02);
2. Užtikrinti duomenų apsaugos procesą, taikant organizacines ir technines kontrolės priemones (žr. 7 pav. valdymo priemonę Nr. 03 ir 04);
3. Nustatyti standartinę saugią konfigūraciją techninėje ir programinėje įrangoje (žr. 7 pav. valdymo priemonę Nr. 04);
4. Griežtai riboti naudotojų, turinčių administratoriaus/privilegijuotas teises, prieigas (žr. 7 pav. valdymo priemonę Nr. 06);
5. Užtikrinti audito žurnalo valdymą ir kontrolę (žr. 7 pav. valdymo priemonę Nr. 08);

6. Tobulinti saugumo supratimo ir kibernetinio saugumo įgūdžius (žr. 7 pav. valdymo priemonę Nr. 14);

7. Užtikrinti incidentų valdymą (žr. 7 pav. valdymo priemonę Nr. 17).

Valdymo priemonės Nr.	KIBERNETINEI GYNYBAI SKIRTOS SAUGUMO KONTROLĖS PRIEMONĖS (CIS Critical Security Controls)	Saugumo priemonių skaičius	IG 1	IG 2	IG 3
01	**Leistinų ir pašalinių įrenginių inventorizavimas** (Inventory and Control of Enterprise Assets)	5	2/5	4/5	5/5
02	**Leidžiamos programinės įrangos inventorizavimas** (Inventory and Control of Software Assets)	7	3/7	6/7	7/7
03	**Duomenų apsauga** (Data Protection)	14	6/14	12/14	14/14
04	**Saugi konfigūracija programinei/techninei įrangai** (Secure Configuration of Enterprise Assets&Software)	12	7/12	11/12	12/12
05	**Paskyrų stebėjimas ir kontrolė** (Account Management)	6	4/6	6/6	6/6
06	**Prieigos valdymas** (Access Control Management)	8	5/8	7/8	8/8
07	**Tęstinis pažeidžiamumų vertinimas ir taisymas** (Continuous Vulnerability Management)	7	4/7	7/7	7/7
08	**Audito įrašų stebėjimas, analizė ir saugojimas** (Audit Log Management)	12	3/12	11/12	12/12
09	**Elektroninio pašto ir naršyklės apsauga** (Email and Web Browser Protections)	7	2/7	6/7	7/7
10	**Apsauga nuo kenksmingo kodo** (Malware Defenses)	7	3/7	7/7	7/7
11	**Duomenų atkūrimo pajėgumai** (Data Recovery)	5	4/5	5/5	5/5
12	**Tinklo infrastruktūros valdymas** (Network Infrastructure Management)	8	1/8	7/8	8/8
13	**Tinklo stebėsena** (Network Monitoring and Defense)	11	0/11	6/11	11/11
14	**Saugumo srities gebėjimų vertinimas ir mokymas** (Security Awareness and Skills Training)	9	8/9	9/9	9/9
15	**Tiekėjų valdymas** (Service Provider Management)	7	1/7	4/7	7/7
16	**Taikomųjų programų saugumas** (Application Software Security)	14	0/14	11/14	14/14
17	**Reagavimas į incidentus ir jų valdymas** (Incident Response Management)	9	3/9	8/9	9/9
18	**Įsibrovimų testavimas** (Penetration Testing)	5	0/5	3/5	5/5
	IŠ VISO SAUGUMO PRIEMONIŲ:	153	56/153	130/153	153

7 pav. 18 kibernetinei gynybai skirtų saugumo kontrolės priemonių sąrašas

Šaltinis: parengta šio darbo autorės pagal CIS Controls modelį (prieiga per internetą: https://www.cisecurity.org/controls/cis-controls-list)

CIS Controls modelis saugumo kontrolės priemones skirsto į tokias kategorijas (grupes):

1. ***Pagrindinė įgyvendinimo grupė*** (angl. *Basic implementation group*, **IG1**). Tai minimalios kibernetinės higienos diegimo priemonių grupė, ją sudaro 56 priemonės (žr. 7 pav.), kurias įgyvendinus žymaus rizikos sumažinimo galima pasiekti nereikalaujant didelių procedūrinių ir (ar) techninių pokyčių. Į šią grupę įeina „7 greiti laimėjimai“, todėl dažnai ekspertų pagal svarbą skirstomos taip: „20% pastangų – 80% rezultato“.

2. ***Papildomų saugumo priemonių įgyvendinimo grupė*** (angl. *Additional Safeguards implementation group*, **IG2**). Tai gilesnės gynybos priemonių įgyvendinimo grupė, ją sudaro 74 papildomos priemonės (kartu su IG1 grupės priemonėmis iš viso – 130 priemonių (žr. 7 pav.)).

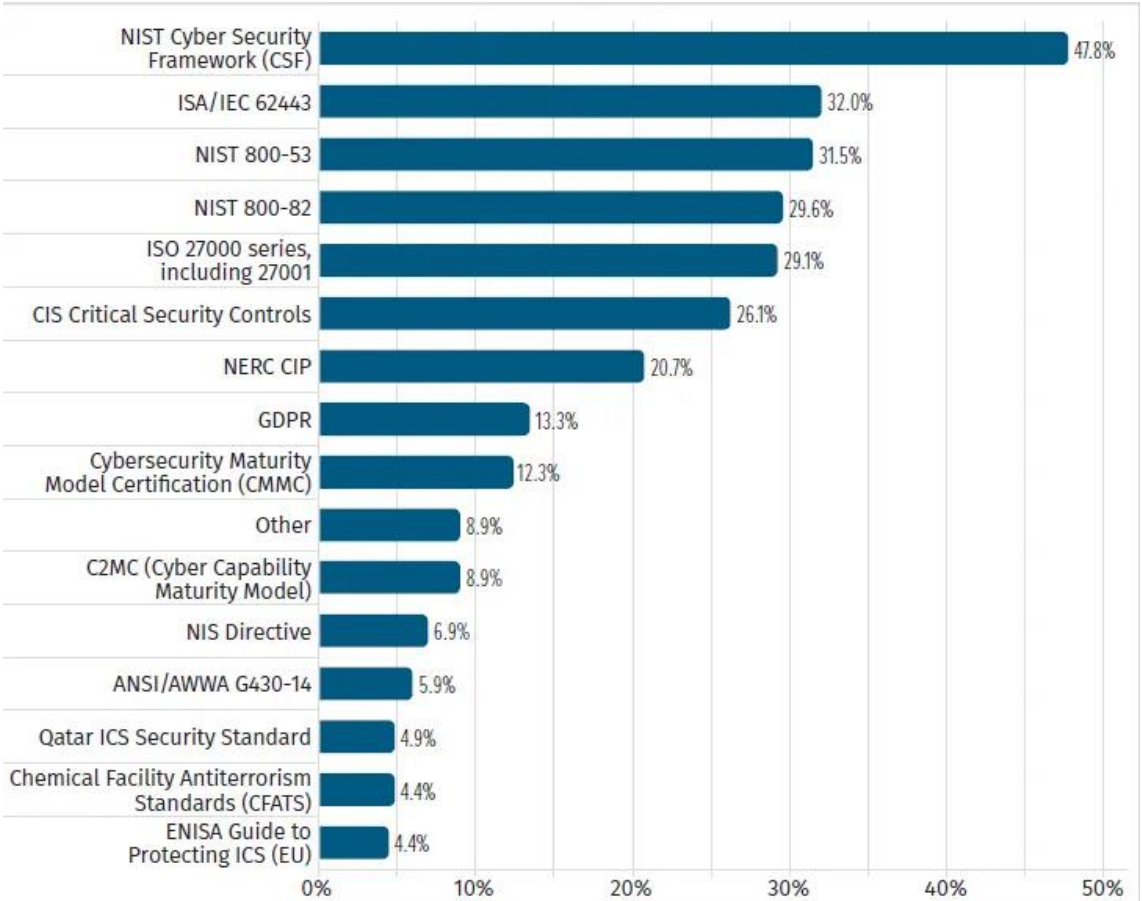
3. ***Pažangios kibernetinės gynybos įgyvendinimo grupė*** (angl. *Advanced Cyber defence implementation group*, **IG3**). Tai maksimizuojančios kibernetinį saugumą priemonės, kurių įgyvendinimui reikalingos investicijos ir pastangos, todėl ekspertų pagal svarbą yra skirstomos taip: "80% pastangų – 20% rezultato". Šią grupę sudaro 23 papildomos priemonės (kartu su IG1 ir IG2 grupių priemonėmis iš viso – 153 priemonės (žr. 7 pav.)).

NKSC, remdamasis SANS instituto ir Kibernetinio saugumo tarybos (angl. *Council on Cyber Security*) gerosios praktikos metodais, periodiškai rengia kibernetinio saugumo gynybai skirtas rekomendacijas, kurios tinka ir mažoms organizacijoms, kurių techninė infrastruktūra ir finansinės galimybės yra nedidelės ir institucijoms, užtikrinančioms kritinės infrastruktūros saugumą. Rekomendacijas galima rasti oficialiame NKSC puslapyje.

Siekiant visuminio požiūrio šiame darbe visos CIS Controls kibernetinei gynybai skirtos priemonės bus vertinamos kuriant objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelį.

1.3.4. Gerosios praktikos metodų palyginimas.

SANS instituto 2021 m. atliktoje kibernetinio saugumo specialistų, dirbančių informacinių technologijų, kibernetinio saugumo valdymo ir informacijos saugumo valdymo srityse apklausa atskleidė kokie standartai yra laikomi geriausiomis praktikomis informacinių sistemų kibernetiniam saugumui vertinti (žr. 8 pav.):



8 pav. 2021 m. geriausios praktikos informacinių sistemų kibernetiniam saugumui vertinti

Šaltinis: SANS 2021 m. apklausos duomenys, prieiga per internetą: https://www.intechww.com/iso-27001-isa-iec-62443-and-nist-csf-selecting-the-right-standard-framework-for-your-ot-cybersecurity-program/)

Lyginant SANS instituto 2021 metais atlikto tyrimo rezultatus su 2019 metais atliktos analogiškos apklausos rezultatais pastebimas augantis NIST CSF standarto populiarumas (žr. 9 pav.).

1	NIST CSF (Cyber Security Framework)	38.1%
2	ISO 27000 series	32.0%
3	NIST 800-53	31.4%
4	NIST 800-82	30.9%
5	ISA/IEC 62443	30.4%
6	CIS Critical Security Controls	29.9%
7	NERC CIP	23.7%
8	GDPR	15.5%
9	C2M2 (Cybersecurity Capability Maturity Model)	10.3%
10	NIS Directive (EU)	8.3%

9 pav. 2019 m. geriausios praktikos informacinių sistemų kibernetiniam saugumui vertinti
Šaltinis: SANS 2019 m. apklausos duomenys, prieiga per internetą https://www.forescout.com/resources/2019-sans-state-of-ot-ics-cybersecurity-survey)

Verta pažymėti, kad tiek NIST CSF tiek ISO/IEC 27001 tiek CIS Controls apima informacijos saugumo užtikrinimą vadovaujantis CIA modeliu. Organizacijoms, siekiančioms turėti dokumentuotą informacinių sistemų kibernetinio saugumo politiką, procesus NIST CSF, ISO/IEC 27001 ir CIS SCF standartai pasiūlo ne tik reikalavimus bet ir rekomendacijas kaip tuos reikalavimus įgyvendinti praktikoje, siekiant atitikties teisės aktuose nustatytiems reikalavimams. Tačiau iš visų standartų tik ISO/IEC 27001 leidžia organizacijai, siekiančios atitikties, atlikti sertifikavimo procesą, t.y. inicijuoti trečiosios šalies vykdomas atitikties standarto reikalavimams vertinimo (organizacijos ISVS audito) procedūras, ir, esant teigiamam vertinimui, gauti tarptautiniu mastu pripažįstamą ISO 27001 sertifikatą.

Lietuvoje informacinių sistemų atitikties teisės aktuose nustatytiems elektroninės informacijos saugos reikalavimams vertinimui atlikti ir stebėsenai vykdyti 2016 m. buvo sukurta ARSIS. Šios informacinės sistemos aplinkoje organizacijoms suteikiama galimybė atlikti informacinių sistemų vertinimus, rizikos analizę pagal ISO/IEC 27001, ISO/IEC 27002 standartų reikalavimus ir (arba) taikant SANS CIS metodą. Tačiau remiantis NKSC duomenimis 2021 m. į ARSIS buvo pateikta tik 19% valstybės informacinių sistemų atitikties elektroninės informacijos saugos ir kibernetinio saugumo reikalavimams ataskaitų (Valstybinio audito ataskaita, 2022). NKSC duomenimis ARSIS nesinaudoja daugelis organizacijų, o kitų priemonių skaitmenizuotai vykdyti saugumo reikalavimų atitiktį ir stebėseną Lietuvoje kol kas nėra sukurta.

Konkretaus gerosios praktikos metodo pasirinkimą įtakoja organizacijos poreikiai, aplinka, kurioje organizacija vykdo savo veiklą, teikia paslaugas. Standartų rekomendacijų įgyvendinimas gali

organizacijai padėti sukurti veiksmingą kibernetinio saugumo aplinką, leidžiančią kovoti su grėsmėmis ir aiškiu, standartizuotu būdu nustatyti pagrindines sritis, skirtas apsaugoti svarbiausią organizacijos infrastruktūrą (Alshar M., 2023). Organizacija gali pasirinkti vieną arba kelis standartus, t.y. kelių gerosios praktikos metodų pagrindu kurti hibridinį, savo organizacijoje taikomą, kibernetinio saugumo modelį, svarbu, kad kibernetinio saugumo politikoje būtų nurodoma kokiais metodais vadovaujantis yra kuriamas informacinės sistemos kibernetinio saugumo valdymas organizacijoje, nes tai suteikia patikimumo tiek organizacijos saugumo politikai, tiek organizacijos valdomoms ir (ar) tvarkomoms informacinėms sistemoms (Harris M. A., 2021).

Mokslininkai (Dzemydienė D., Naujikienė R., 2016, Harris M. A., 2021) pažymi, kad pasirenkant gerosios praktikos metodus, priemones, sprendimus, verta taip pat įvertinti šiuos aspektus:

1. daugelio saugumo priemonių naudojimas, ypač tokių, kurios įtakoja naudotojo elgesį, gali neigiamai įtakoti bendrą saugumo situaciją organizacijoje dėl informacinių sistemų naudotojų pasipriešinimo, kuris dažnai yra susijęs su priemonių naudojimo „nepatogumu“ naudotojams arba saugumo politikos „neaiškumu“. Todėl būtina nuolat mokyti personalą, ugdyti jo sąmoningumo lygį, supažindinti su kylančiomis grėsmėmis ir apsaugos priemonių būtinumu. Darbuotojai turi suprasti savo atsakomybės dalį informacinių sistemų kibernetinio saugumo užtikrinimo procese.

2. Ekonomiškai vertinant informacinių sistemų kibernetinio saugumo sprendimui taikomų priemonių efektyvumą, reiktų atsižvelgti į tai, kad per didelės investicijos, neproporcingi technologiniai ir organizaciniai sprendimai gali tapti tokių saugumo sprendimų neveiksnumo priežastimi, o investicijos į tokias kibernetinio saugumo priemones gali virsti bevertėmis pastangomis, nenaudojamu turtu.

1.3.5. Lietuvos teisės aktuose nustatytų reikalavimų, taikomų informacinių sistemų kibernetinio saugumo vertinimo procesui, analizė

Lietuvoje informacinių sistemų saugumą reglamentuoja virš 20 skirtingų teisės aktų. Visus juos galima būtų suskirstyti į 2 kategorijas:

1. Valstybės informacinių išteklių saugumą reglamentuojantys teisės aktai.

2. Kibernetinį saugumą reglamentuojantys teisės aktai.

Prie pirmos kategorijos teisės aktų priskirtini visi teisės aktai, kurie susiję su Lietuvos Respublikos Valstybės informacinių išteklių valdymo įstatymu ir jo įgyvendinimu. Prie antros kategorijos teisės aktų priskirtini visi teisės aktai, kurie susiję su Lietuvos Respublikos Kibernetinio saugumo įstatymu ir jo įgyvendinimu. Pagrindiniai teisės aktai, reglamentuojantys valstybės informacinių sistemų ir jose tvarkomos elektroninės informacijos saugumą ir kibernetinį saugumą nurodyti 2 lentelėje.

2 lentelė Teisės aktų, reglamentuojančių valstybės informacinių sistemų, jose tvarkomos elektroninės informacijos saugumą ir kibernetinį saugumą, sąrašas

Eil. Nr.	Valstybės informacinių išteklių saugumą reglamentuojantys teisės aktai	Kibernetinį saugumą reglamentuojantys teisės aktai
1.	Valstybės informacinių išteklių valdymo įstatymas (LRĮ XI-1807, 2011)	Kibernetinio saugumo įstatymas (LRĮ, XII-1428, 2014)
2.	Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašas (LRV Nr. 180, 2013)	Ypatingos svarbos informacinės infrastruktūros identifikavimo metodika (LRV Nr. 818, 2018)
3.	Bendrųjų elektroninės informacijos saugos reikalavimų aprašas (LRV Nr. 716, 2013)	Nacionalinis kibernetinių incidentų valdymo planas (LRV Nr. 818, 2018)
4.	Saugos dokumentų turinio gairių aprašas (LRV Nr. 716, 2013)	Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas (LRV Nr. 818, 2018)
5.	Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas (LRV Nr. 716, 2013)	Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašas (KAM įsakymas Nr. V-941, 2020)
6.	Valstybės informacinių sistemų gyvavimo ciklo valdymo metodika	Informacinių technologijų saugos atitikties vertinimo metodika (KAM įsakymas Nr. V-941, 2020)

Šaltinis: parengta šio darbo autorės

Dėl nuolatinių pokyčių Lietuvos informacinių išteklių ir kibernetinio saugumo politikos formavimo ir valdymo srityje, kurie trūko nuo 2013 m. iki 2018 m., t. y. kuomet atsakomybė už Lietuvos Respublikos valstybės informacinių išteklių politikos formavimą buvo pakankamai diferencijuota, sutelkta ,,skirtingose rankose“ (pvz., informacinių sistemų saugumo politikos formavimo funkcijas vykdė Vidaus reikalų ministerija, Susisiekimo ministerija, Ūkio ministerija, Krašto apsaugos ministerija, Informacinės visuomenės plėtros komitetas), Lietuvoje nepavyko pasiekti konsoliduoto, sisteminio teisinio reglamentavimo informacinių sistemų valdymo ir kibernetinio saugumo srityje. Apie tai pažymima 2022 m. valstybinio audito ataskaitoje. Pažymėtina, kad apie būtinybę turėti holistines teisinio reguliavimo priemones dar 2011 m. rašė Lietuvos mokslininkai (Štitilis D., Pakutinskas P., 2011). Deja, bet 2023 metais organizacijai, siekiančiai įvertinti savo valdomų ir (ar) tvarkomų informacinių sistemų saugumą ir atitiktį Lietuvos teisės aktuose nustatytiems kibernetinio saugumo reikalavimams, atliekant kibernetinio saugumo vertinimus ir atitikties vertinimus, vis dar reikia kompleksiškai taikyti tiek informacinių išteklių saugumą reglamentuojančius teisės aktus tiek kibernetinį saugumą reglamentuojančius teisės aktus.

Informacinių sistemų kibernetinis saugumas užtikrinamas iš esmės įgyvendinant organizacinius ir techninius kibernetinio saugumo reikalavimus (toliau – Reikalavimai). Vadovaujantis Organizacinių ir techninių reikalavimų aprašo 9 punktu valstybės informacinių sistemų valdytojai ir (ar) tvarkytojai ne rečiau kaip kartą per metus turi organizuoti ir atlikti informacinių sistemų atitikties Reikalavimams vertinimą (toliau – atitikties KS reikalavimams vertinimas). Pagal Techninių reikalavimų aprašo 5.1. papunktį informacinės sistemos informacinių technologijų saugos atitikties vertinimas (toliau – Saugos atitikties vertinimas) turi būti atliekamas ne rečiau kaip 1 (vieną) kartą per dvejus metus

(antros ir aukštesnės kategorijos informacinėms sistemoms – ne rečiau kaip kartą per metus). Saugos atitikties vertinimas turi būti atliekamas vadovaujantis Informacinių technologijų saugos atitikties vertinimo metodika, o atitikties kibernetinio saugumo reikalavimams vertinimas – vadovaujantis Organizacinių ir techninių reikalavimų aprašu. Organizacijoms, siekiančioms objektyviai nustatyti saugos reikalavimų įgyvendinimo lygį rekomenduojama vertinimo metu atlikti tokias veiklas, nurodytas Informacinių technologijų saugos atitikties vertinimo metodikos 5.1–5.6. papunkčiuose:

1. informacinės sistemos techninės ir programinės įrangos inventorizaciją;
2. ne mažiau kaip 10 % atsitiktinai parinktų informacinės sistemos naudotojų darbo vietų patikrinimą, informacinės sistemos tarnybinėse stotyse įdiegtos programinės įrangos ir jų sąrankos aktualumo patikrinimą;
3. informacinės sistemos naudotojams suteiktų teisių ir naudotojų vykdomų funkcijų atitikties patikrinimą;
4. pasirengimo užtikrinti informacinės sistemos veiklos tęstinumą vertinimą (pvz., įvykus elektroninės informacijos saugos incidentui);
5. informacinės sistemos rizikos įvertinimą ir valdymo būklės patikrinimą;
6. informacinės sistemos saugos dokumentų kokybės patikrinimą (pvz. ar dokumentai peržiūrimi saugos reikalavimuose nustatytu dažnumu).

Verta pažymėti, kad vienas iš atitikties kibernetinio saugumo reikalavimams vertinimo elementų – pažeidžiamumų vertinimo procesas yra glaudžiai susijęs su kitu reikalavimu, taikomu projektams, kuriuos įgyvendinant organizacijos kuria naujas elektronines paslaugas arba modernizuoja jau sukurtas elektronines paslaugas, įskaitant sudėtines elektronines paslaugas. Vadovaujantis Elektroninių paslaugų kūrimo metodikos (toliau – Elektroninių paslaugų kūrimo metodika) 29 punktu tuo atveju, kai yra sukuriamos ar modernizuojamos elektroninės paslaugos, būtina patikrinti:

1. sukurtų paslaugų atsparumą įsilaužimui,
2. galutinių elektroninių paslaugų naudotojų darbo vietas;
3. naudotojų atsparumą socialinei inžinerijai.

Elektroninių paslaugų kūrimo metodikoje nurodoma, kad atliekant atsparumą įsilaužimams „turi būti tikrinamas išorinio sistemos kompiuterių tinklo perimetras, vidinio kompiuterinio tinklo infrastruktūra, tarnybinių stočių saugumas, sistemos tvarkytojų darbo vietų saugumas, kt. Patikrinimą turi atlikti nuo elektroninių paslaugų kūrimą vykdančio subjekto (diegėjo) nepriklausomas paslaugų teikėjas“ (Elektroninių paslaugų kūrimo metodika, 2015).

Taigi iš esmės net 3 (trys) teisės aktai įpareigoja informacinių sistemų valdytojus nustatytu periodiškumu ir pagal poreikį (pvz. kai atliekamos valstybės informacinės vystymo, modernizavimo paslaugos, kuriamos naujos elektroninės paslaugos) atlikti informacinių sistemų, sukurtų elektroninių paslaugų atitikties kibernetinio saugumo reikalavimams vertinimą, patikrinti informacinės sistemos

silpnąsias vietas, atlikti technologinio pažeidžiamumų (angl. *penetration testing*) vertinimą, numatyti atitinkamas valdymo priemones nustatytiems trūkumams (neatitiktims) pašalinti.

Svarbu pažymėti, kad 2022 m. atlikto valstybinio audito ataskaitoje nurodyta, kad „atlikus kibernetinį saugumą ir elektroninės informacijos saugą reglamentuojančių teisės aktų palyginimą su ISO/IEC 27001 standarto reikalavimais, buvo nustatyta, kad informacijos, kibernetinio saugumo valdymo politika ir saugos kontrolės priemonės Lietuvos nacionalinėje teisėje parengti pagal šio standarto rekomendacijas. Nustatyti organizaciniai ir techniniai saugumo valdymo reikalavimai atitinka šios srities gerąsias praktikas“ (Valstybinio audito ataskaita, 2022).

Atlikus detalesnį Lietuvoje galiojančio teisinio reglamentavimo analizę pastebėta, kad tik pirmos kategorijos valstybės informacinės sistemos, jų valdytojai turi įgyvendinti gerosios praktikos standartuose ISO/IEC 27001 ir ISO/IEC 27002 nurodytus ISVS keliamus reikalavimus. ISVS atitiktis ISO/IEC 27001 standarto reikalavimams vertinimas turi būti atliekamas ne rečiau kaip kartą per 3 (trejus) metus, o patį atitikties vertinimą informacinės sistemos valdytojas ir (ar) tvarkytojas turi patikėti atlikti nepriklausomiems, visuotinai pripažintiems, tarptautinių organizacijų sertifikuotiems informacinių sistemų auditoriams. Toks reikalavimas nėra taikoma antros ir žemesnės kategorijos informacinėms sistemoms, jų valdytojams ir (ar) tvarkytojams, vidaus administravimui skirtoms informacinėms sistemoms (pvz. dokumentų valdymo sistemoms).

Atlikus detalesnį NKSC teikiamų kibernetinio saugumo paslaugų sąrašo, sudaryto atsižvelgiant į kibernetinio saugumo įstatymu ir kitais teisės aktais NKSC priskirtų funkcijų vykdymą ir remiantis tarptautine FIRST organizacijos praktika, pastebėta, kad technologinio pažeidžiamumo (angl. k. *penetration testing*) NKSC atlieka tik YSII valdytojų atžvilgiu.

Tai, kad Lietuvos Respublikos teisės aktuose atitiktis ISO/IEC 27001 standarto reikalavimams yra iš esmės privaloma tik pirmos kategorijos valstybės informacinėms sistemoms ir YSII yra labai svarbus aspektas vertinant galimą skirtingą valstybės informacinių sistemų valdytojų ir (ar) tvarkytojų, kaip organizacijų, požiūrį į pasirengimą užtikrinti informacinių sistemų kibernetinį saugumą ir atitiktį teisės aktuose nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams. Manytina, kad pirmos kategorijos informacinių sistemų valdytojų ir (ar) tvarkytojų požiūris į tarptautinių standartų taikymą organizacijos veikloje ir jų įtaka informacinės sistemos kibernetiniam saugumui turėtų būti teigiamas, nes gerosios praktikos metodai turėtų būti taikomi organizuojant šių organizacijų informacijos saugumo valdymo procesus, atliekant informacinių sistemų kibernetinio saugumo vertinimus.

Atsižvelgiant į tai galima kelti hipotezę: gerosios praktikos metodai turi teigiamą įtaką informacinės sistemos kibernetiniam saugumui ir visos organizacijos kibernetiniam saugumui.

2. INFORMACINĖS SISTEMOS KIBERNETINIO SAUGUMO VERTINIMO TYRIMO METODOLOGIJA

2.1. Tyrimo objekto pristatymas.

Šiame magistro baigiamajame darbe analizuojamas informacinės sistemos kibernetinio saugumo vertinimo procesas. Informacinės sistemos kibernetinis saugumas – tai jos gebėjimas būti atspariai bet kokiam informacijos saugumo įvykiui, bet kokiai grėsmei, kuri gali kilti kibernetinėje erdvėje ir informacinės sistemos veikimo (funkcionavimo) ribose. Informacinės sistemos kibernetinis saugumas turi būti vertinamas atsižvelgiant į grėsmes, kylančias informacijos, saugomos informacinėje sistemoje, saugumui (konfidencialumui, vientisumui ir prieinamumui) viso informacinės sistemos gyvavimo ciklo metu (žr. 1 pav.). Informacinės sistemos kibernetinio saugumo vertinimo procesas turėtų apimti bent tokias informacinės sistemos kibernetinio saugumo vertinimo veiklas kaip rizikų vertinimas (grėsmių ir pažeidžiamumų vertinimas), saugumo valdymo priemonių (teisinių, organizacinių, techninių, fizinių) vertinimą, informacinės sistemos veikimo (funkcionavimo) aplinkos saugumo, technologinio pažeidžiamumo (angl. *penetration testing*) ir socialinės inžinerijos pažeidžiamumo (angl. *Social Engineering Penetration Test*) vertinimus. Siekiant visapusiško ir objektyvaus informacinės sistemos kibernetinio saugumo vertinimo, informacinės sistemos vertinimo procese turi dalyvauti skirtingų žinių ir kompetencijų specialistai, vertinimo procesas turi būti atliekamas vadovaujantis gerąja praktika, taikant gerosios praktikos metodus.

Informacinės sistemos saugumo lygis tiesiogiai įtakoja kibernetinio saugumo priemonių parinkimą ir taikymą. Kokius reikalavimus turi tenkinti informacinė sistema paprastai nustatoma teisės aktuose. Kaip, t. y. kokius metodus ir kokias priemones (organizacines, technines, fizines) taikant užtikrinamas informacinės sistemos kibernetinis saugumas priklauso nuo organizacijos, kurį valdo ir (ar) tvarko informacinę sistemą kibernetinio saugumo valdymo brandos. 2023 m. vasario 28 d. duomenimis Registrų ir valstybės informacinių sistemų registre buvo registruota 313 informacinių sistemų ir 94 registrų, kuriuos valdo 151 skirtingų valdytojų ir 172 skirtingų tvarkytojų. 2021 m. – 2022 m. I ketvirčio NKSC duomenimis daugelis informacinių sistemų valdytojų ir (ar) tvarkytojų kibernetinio saugumo reikalavimus savo valdomose ir (ar) tvarkomose informacinėse sistemose įgyvendino formaliai. Toks formalus požiūris į informacinių sistemų kibernetinį saugumą nesikeičia Lietuvoje nuo 2016 metų. Apie tai pažymima 2022 m. NKSC Nacionalinėje kibernetinio saugumo būklės ataskaitoje, 2022 m. Valstybinio audito ataskaitoje ir 2021–2027 m. Visuomenės skaitmeninimo išankstinio poveikio vertinimo paslaugų ataskaitoje.

2.2. Tyrimo tikslingumo pagrindimas

Mokslinės literatūros ir mokslinių tyrimų analizė atskleidė, kad informacinių sistemų kibernetinio saugumo vertinimas ir informacinių sistemų atitikties kibernetinio saugumo reikalavimams procesas analizuojamas tiek Lietuvos tiek užsienio mokslininkų jau daugiau kaip 10 metų. Mokslininkai pagrindžia mintį, kad informacinės sistemos kibernetinio saugumo vertinimas ir kibernetinio saugumo įgyvendinimas (atitiktis teisės aktuose nustatytiems reikalavimams) apima įvairias problemines sritis – techninę, teisinę, finansinę, vadybos (organizacinę) ir žmogiškąją (Leger M.A. 2022), o tokie faktoriai kaip organizacijos kontekstas (Marotta A., Madnick S., 2021), informacinių ir pramoninių sistemų projektavimo spragos (Qassim Q., Jamil N., 2019), technologinis pažeidžiamumas, žmogiškasis veiksnys (Harrel M. N., 2014), teisės aktuose nustatyto teisinio reglamentavimo trūkumai (Al-hashimi, M., Othman, 2018, Štitilis D., Pakutinskas P., 2011) turi įtakos organizacijos valdomų informacinių sistemų kibernetiniam saugumui. Mokslininkai pabrėžia, kad tarptautiniai standartai ir metodai yra tvirtas pagrindas atlikti informacinių sistemų kibernetinio saugumo vertinimus vadovaujantis gerąja praktika tiek kritinės infrastruktūros valdytojams (Roshanaei M., 2021) tiek mažoms ir vidutinėms įmonėms (Venkatech V., 2018), standartai puikiai pritaikomi valstybėms kuriant nacionalines kibernetinio saugumo sistemas (Angelini M., Ciccotelli C. 2020). Vieni mokslininkai (Fathi S., Hikal N., 2019) laikosi nuomonės, kad informacinės sistemos kibernetinio saugumo vertinimo procesas turi būti grindžiamas technologinio pažeidžiamumo (angl. *penetration testing*) vertinimo metodais, kitų mokslininkų (Leger M.A., 2022) nuomone informacinės sistemos kibernetinis saugumas priklauso nuo to kaip organizacija užtikrina atitiktį kibernetinio saugumo reikalavimams, t.y. kaip valdo informacinės sistemos atitiktį kibernetinio saugumo reikalavimams. Dalis mokslininkų (Harris M. A, Martin R., 2021, Štitilis D., 2021, Hassan A., Binti A., 2022) savo tyrimuose išskiria informacinių sistemų neatitikties (angl. *noncompliance*), kibernetinio saugumo reikalavimams problematiką arba kitaip dar vadinamą formalios atitikties problematiką. Pagal Harris M. A, tik sukūrus ir taikant veiksmingą teorinį ir technologinį (automatizuotą) informacinės sistemos kibernetinio saugumo vertinimo modelį, galima būtų organizacijai objektyviai atlikti informacinės sistemos kibernetinio saugumo vertinimą, maksimaliai atitikti kibernetinio saugumo reikalavimus (Harris M.A., 2021). Toks modelis galėtų išspręsti subjektyvaus, formalaus, informacinės sistemos kibernetinio saugumo vertinimo problemą, kuri šiai dienai neturi sprendimo.

Informacinių sistemų kibernetinis saugumas vis labiau yra ne tik organizacijos, bet ir kiekvienos valstybės nacionalinio saugumo klausimas (Baldini G. Barrero J., 2020). Nuo 2020 m. kibernetinio saugumo incidentų ir duomenų saugumo pažeidimų, dėl kurių pasaulio valstybės patiria nuostolius, kasmet tik didėja (Ponemon Institute, IBM Security, 2022). Todėl informacinės sistemos kibernetinis saugumas ir informacinės sistemos atitiktis teisės aktuose nustatytiems kibernetinio saugumo

reikalavimams problematika įgyja didesnį aktualumą ir reikalauja išskirtinio dėmesio. Holistinis (visuminis) požiūris šioje srityje yra būtinas tiek taikant aiškesnes sistemingesnes holistines teisinio reguliavimo priemones (Štitilis D., Pakutinskas P., 2011), tiek sistemiškai vertinant rizikas (Kandsamy K, Srinivas S., 2020) tiek diegiant holistinį (visuminį) požiūrį į Lietuvos kibernetinį saugumą, įgyvendinant 2021–2027 m. Ekonomikos gaivinimo ir atsparumo didinimo plane „Naujos kartos Lietuva“ numatytas kibernetinio saugumo priemones (pvz., sukurti nacionalinę kibernetinio saugumo valdymo sistemą, Organizacinių ir techninių kibernetinio saugumo reikalavimų nacionalinės stebėsenos sistemos skaitmeninį sprendimą).

Tyrimo problema – Kaip, taikant šiuolaikinius mokslinius ir gerosios praktikos metodus objektyviai atlikti informacinės sistemos kibernetinio saugumo vertinimą?

Tyrimo tikslas – sukurti informacinės sistemos kibernetinio saugumo vertinimo modelį ir pateikti siūlymus objektyviam informacinių sistemų kibernetinio saugumo vertinimui atlikti.

Tyrimo hipotezė – gerosios praktikos metodai turi teigiamą įtaką informacinės sistemos kibernetiniam saugumui ir visos organizacijos kibernetiniam saugumui.

Tyrimo uždaviniai:

1. Išanalizuotos mokslinės literatūros, teorinių strategijų, tarptautinės gerosios praktikos, Europos Sąjungos, Lietuvos tesės aktuose nustatytų reikalavimų, taikomų informacinių sistemų kibernetinio saugumo vertinimo procesui, pagrindu identifikuoti pagrindinius teorinius informacinės sistemos kibernetinio saugumo vertinimo modelio aspektus.
2. Sukurti objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelį.
3. Atlikti kokybinį tyrimą, kurio pagrindu galima būtų įvertinti sukurto informacinės sistemos kibernetinio saugumo vertinimo modelį, identifikuoti neatitikties (formalios atitikties) atsiradimo priežastis, numatyti (pasiūlyti) gerinimo priemones.
4. Įvertinti sukurto informacinės sistemos kibernetinio saugumo vertinimo modelio taikymo praktikoje galimybes, pateikti siūlymus dėl objektyvaus informacinės sistemos kibernetinio saugumo vertinimo proceso tobulinimo krypčių.

2.3. Kokybinio tyrimo metodų pagrindimas ir apibūdinimas.

Teoriniai metodai: Siekiant suformuluoti informacinės sistemos kibernetinio saugumo vertinimo modelio teorinį pagrindą buvo vykdoma sisteminė mokslinės literatūros, mokslinių tyrimų, gerosios praktikos metodų (pvz. ISO/IEC, NIST, CIS Controls), Europos Sąjungos ir Lietuvos Respublikos teisės aktų, valstybės informacinių sistemų saugos politiką, kibernetinį saugumą ir atitikties kibernetinio saugumo reikalavimams reglamentuojančių juridinių ir kitų dokumentų kokybinė turinio analizė (angl. k. *Content analysis*).

Empiriniai metodai: Informacinės sistemos kibernetinio saugumo vertinimo modeliui kurti ir sukurto modelio validacijai pasirinkti vienas kitą papildantys kokybiniai empiriniai tyrimai:

1. **atvejo analizė** (anglų k. *Case study*). Pagal Kalibatienę D. ir Simanavičienę R, šis metodas mokslinėje literatūroje yra rekomenduojamas tais atvejais, kai siekiama ištirti vieną šiuolaikinio informatikos mokslų reiškinį, nustatyti pagrindinius veiksnius, galinčius turėti įtakos veiklai (Kalibatienė D, Simanavičienė R., 2021). Šiame darbe nagrinėjamas informacinės sistemos kibernetinio saugumo vertinimo procesas, kaip reiškinys, išgryninami pagrindiniai vertinimo proceso elementai, identifikuojama vertinimo imtis, nustatomi veiksniai, turintys įtakos neatitikties (angl. *noncompliance*) kibernetinio saugumo reikalavimams atsirasti.

2. **kokybinė turinio analizė** (angl. *Content analysis*) – atvejo analizei (angl. *Case study*) reikalingiems pirminiams duomenims (angl. *Primary data*) surinkti atliekama juridinių ir kitų, viešai prieinamų, pvz. Registrų ir valstybės informacinių sistemų registre skelbiamos informacijos, prieiga per internetą: https://registrai.lt/login, valstybės informacinių sistemų saugos ir kitų dokumentų turinio analizė bei antrinių duomenų (anglų k. *Secondary data)*, t.y. kitų mokslinių tyrimų surinktų duomenų analizė (pagal Kalibatienę D, Simanavičienę R., 2021).

3. **Ekspertinė kokybinė** iš dalies struktūruota (angl. *Semi-structured*) **apklausa** (pagal Gaižauskaitę I., Valavičienę N., 2016).

Ekspertinei kokybinei apklausai ekspertais (ne mažiau kaip N=10) pasirinkti:

1. valstybės informacinių sistemų saugos įgaliotiniai, kibernetinio saugumo vadovai, kurie atlieka tiriamųjų valstybės informacinių sistemų valdytojų ir (ar) tvarkytojų (nurodyti 3 lentelėje) valdomų ir (ar) tvarkomų valstybės informacinių sistemų saugos įgaliotinio ir (ar) atsakingo už informacinių sistemų kibernetinį saugumą asmens funkcijas. Ekspertu laikytinas asmuo, kuris turi ne mažesnę kaip 3 metų patirtį vykdant saugos įgaliotinio funkcijas ir (arba) atsakingo už informacinės sistemos kibernetinį saugumą asmens funkcijas, t.y. turi patirties organizuojant (atliekant) informacinių sistemų atitikties kibernetinio saugumo reikalavimams vertinimus, rizikos vertinimus.

2. NKSC specialistai, kurie atlieka valstybės informacinių sistemų atitikties teisės aktuose nustatytiems elektroninės informacijos saugos reikalavimams vertinimo ir stebėsenos funkcijas, derina informacinių sistemų valdytojų ir (ar) tvarkytojų parengtus saugos dokumentų projektus, konsultuoja informacinių sistemų valdytojus ir (ar) tvarkytojus saugos klausimais, atlieka organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimo stebėseną, pažeidžiamumų vertinimą (toliau – kibernetinio saugumo paslaugos). Ekspertu laikytinas asmuo, kuris turi ne mažesnę kaip 3 metų patirtį teikiant kibernetinio saugumo paslaugas.

Sudarant kokybinės apklausos ekspertų imtį (ekspertų skaičius turėtų būti ne mažesnis kaip N=10) buvo vadovaujamasi Balžentis A. ir Žalimaitė M. atlikto tyrimo, kuriame buvo pateiktos išvados, kad atliekant kokybinius vertinimus ekspertų skaičius gali būti mažesnis nei 7-10 ekspertų

(Balžentis A., Žalimaitė M., 2011). Atsižvelgiant į tai, laikytina, kad atliekant tyrimą informacijos saugos įgaliotinių ir (ar) informacinių sistemų kibernetinės saugos specialistų skaičius kartu su NKSC ekspertais, teikiančiais kibernetinio saugumo paslaugas, turėtų būti ne mažesnis kaip 10, tokia imtis kokybiniam tyrimui yra pakankama.

Ekspertinei kokybinei apklausai ekspertų organizacijų pasirinkimo imtis. Tyrimo imčiai pagrįsti taikyta netikimybinė tikslinė atranka. Tiriamųjų valstybės informacinių sistemų valdytojų ir (ar) tvarkytojų (žr. 3 lentelę) organizacijos pasirinktos remiantis šiais atrankos kriterijais:

1. Informacinės sistemos valdytojas ir (ar) tvarkytojas turi būti institucija, atitinkanti Valstybės informacinių išteklių valdymo įstatymo 1 straipsnio 3 dalies reikalavimus;

2. Informacinės sistemos valdytoja ir (ar) tvarkytoja turi turėti ne mažiau kaip 2 (dvi) valstybės informacines sistemas ir (ar) registrus;

3. Informacinės sistemos valdytoja ir (ar) tvarkytoja turi turėti ne mažiau kaip 1 (vieną) pirmos kategorijos valstybės informacinę sistemą ir (ar) registrą arba YSII priskirtą informacinę sistemą, t. y. valdyti ir (ar) tvarkyti bent 1 (vieną) informacinę sistemą, kuriai taikomi reikalavimai dėl atitikties ISO/IEC 27001 standarto reikalavimams pagal Techninių reikalavimų aprašo 8.3 papunktį.

Detalus tiriamųjų valstybės informacinių sistemų valdytojų ir tvarkytojų sąrašas, parengtas pagal Registrų ir valstybės informacinių sistemų registre (prieiga per internetą: https://registrai.lt/login) registruotus objektus, šio darbo 4 priede ,,Informacija apie Registrų ir valstybės informacinių sistemų registre registruotus objektus, jų valdytojus“ pateiktą informaciją ir pagal tyrimo imčiai nustatytus atrankos kriterijus, kurie detaliai nurodyti 3 lentelėje. Atrankos metu Registrų ir valstybės informacinių sistemų registre (tikrinta 2023 m. vasario 28 d.) buvo registruota 313 informacinių sistemų ir 94 registrų, kuriuos valdo 151 skirtingų valdytojų ir 172 skirtingų tvarkytojų. NKSC pasirinkta atsižvelgiant į tai, kad šiai organizacijai yra priskirtos funkcijos, susijusios su organizacinių ir techninių reikalavimų įgyvendinimo stebėsena, informacinių sistemų saugos dokumentų derinimu, kibernetinio saugumo pažeidžiamumų valdymu (žr. detalų NKSC teikiamų paslaugų sąrašą, skelbiamą šiuo adresu: https://www.nksc.lt/paslaugos.html).

3 lentelė Tiriamųjų valstybės informacinių sistemų valdytojų ir (ar) tvarkytojų sąrašas

Eil. Nr.	Valstybės informacinės sistemos valdytojo ir (ar) tvarkytojo pavadinimas	Atitiktis VIIVĮ 1 str. 3d. reikala-vimams (taip / ne)	Valdomų /tvarkomų valstybės informacinių sistemų skaičius	Yra bent vienos Pirmos kategorijos informacinės sistemos ar YSII valdytojas (taip/ne)	Nuoroda į duomenų saugos nuostatų punktus, papunkčius, kuriuose nustatyta kokiai kategorijai priklauso informacinė sistema, registras ir (ar) informacinė infrastruktūra
1.	Ekonomikos ir inovacijų ministerija / ***Informacinės visuomenės plėtros komitetas***	Taip	13	Taip	Valstybės informacinių išteklių sąveikumo platformos duomenų saugos nuostatų, patvirtintų Ekonomikos ir inovacijų ministro 2021 m. rugpjūčio 9 d. įsakymu Nr. 4-886, 19 p. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/f5049700f90a11eb9f09e7df20500045 (tikrinta 2023-02-28)

3 lentelės tęsinys kitame puslapyje

3 lentelės tęsinys

2.	Ekonomikos ir inovacijų ministerija / ***Valstybės įmonė Registrų centras***	Taip	25	Taip	Valstybės įmonės Registrų centro tvarkomų registrų ir informacinių sistemų duomenų saugos nuostatų, patvirtintų Teisingumo ministro 2017 m. gegužės 22 d. įsakymu Nr. 1R-132 23.1 papunktis Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/83cc93a03eb311e7b66ae890e1368363/asr (tikrinta 2023-02-28)
3.	***Užsienio reikalų ministerija***	Taip	4	Taip	Lietuvos Respublikos (toliau – LR) užsienio reikalų ministerijos informacinių sistemų duomenų saugos nuostatai, patvirtinti LR užsienio reikalų ministro 2022 m. vasario 23 d. įsakymu Nr. V-54, 16.2 papunktis (tikrinta 2023-02-28)
4.	Finansų ministerija / ***Valstybinė mokesčių inspekcija***	Taip	13	Taip	Valstybinės mokesčių inspekcijos informacinių sistemų duomenų saugos nuostatų, patvirtintų Valstybinės mokesčių inspekcijos prie LR Finansų ministerijos viršininko 2021 m. liepos 20 d. įsakymu Nr. V-281, 17.1 papunktis (tikrinta 2023-02-28)
5.	Finansų ministerija / ***Muitinės departamentas***	Taip	2	Taip	Muitinės informacinių sistemų duomenų saugos nuostatų, patvirtintų Muitinės departamento prie LR Finansų ministerijos generalinio direktoriaus 2019 m. rugsėjo 16 d. įsakymu Nr. 1B-824 1 priedas, Prieiga per internetą: 1B-824 Dėl Muitinės departamento prie Lietuvos Respublikos finansų ministerijos generalinio direktoriaus... (e-tar.lt),(tikrinta 2023-02-28)
6.	Vidaus reikalų ministerija / ***Informatikos ir ryšių departamentas***	Taip	21	Taip	Kai kurių Vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų duomenų saugos nuostatų, patvirtintų Vidaus reikalų ministro 2017 m. gruodžio 22 d. įsakymu Nr. 1V-883 priedas, Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/b21aa380e71111e7acd7ea182930b17f/asr (tikrinta 2023-02-28)
7.	Krašto apsaugos ministerija/ ***Kertinis valstybinis telekomunikacijų centras***	Taip	4	Taip	Saugaus valstybinio duomenų perdavimo tinklo saugos nuostatų, patvirtintų Lietuvos Respublikos Krašto apsaugos ministro 2018 m. vasario 7 d. įsakymu Nr. V-135 patvirtinti 17 punktas, Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/f3b8f1300bff11e8a5fc9d9b3a58917b, (tikrinta 2023-02-28)
8.	Aplinkos ministerija / ***Valstybinė miškų tarnyba***	Taip	25	Taip	LR miškų valstybės kadastro duomenų saugos nuostatų, patvirtintų LR Aplinkos ministro 2014 m. gruodžio 31 d. įsakymu Nr. bD1-1093, 13 punktas, Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/b642eea090ce11e4bb408baba2bdddf3 (tikrinta 2023-02-28)

Šaltinis: parengta šio darbo autorės pagal Registrų ir valstybės informacinių sistemų registre skelbiamą informaciją (prieiga per internetą: https://registrai.lt/login), tikrinta 2022-02-28

2.4. Tyrimo dizainas ir rezultatų patikimumas.

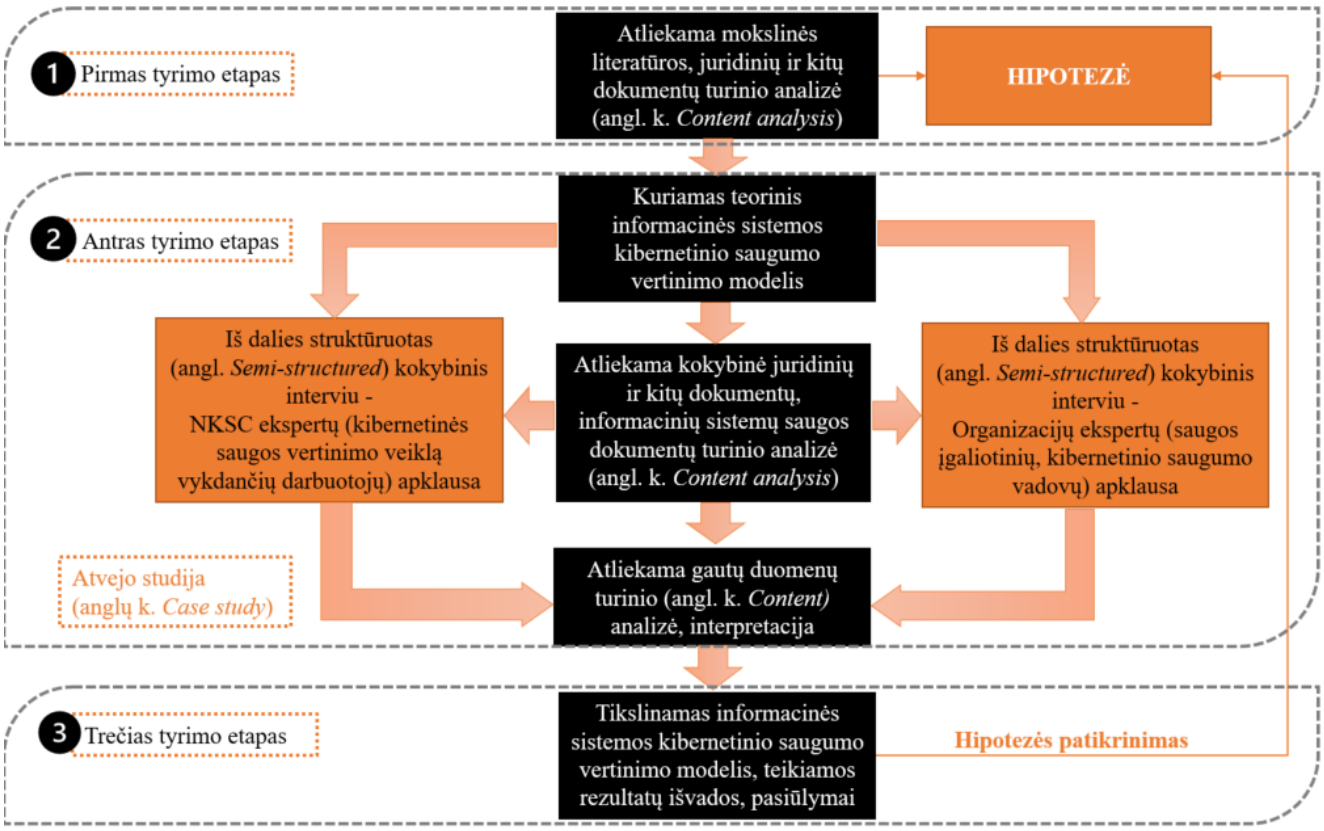
Siekiant užtikrinti sėkmingą tyrimo įgyvendinimą, sudaromas detalus tyrimo planas, kuriame numatomas tyrėjo veiksmų ir veiklos eiliškumas. Tyrimo planą sudaro trys pagrindiniai etapai:

Pirmajame etape siekiant suformuluoti informacinės sistemos kibernetinio saugumo vertinimo modelio teorinį pagrindą sistemiškai analizuojama mokslinė literatūra, teorinės informacinių sistemų kibernetinio saugumo vertinimo proceso apimties koncepcijos, nagrinėjami gerosios praktikos metodai (ISO/IEC, NIST, CIS Controls), jų privalumai ir trūkumai, atliekama Europos Sąjungos ir Lietuvos nacionaliniuose teisės aktuose nustatyti reikalavimai informacinių sistemų kibernetinio saugumo vertinimo ir atitikties kibernetinio saugumo reikalavimams vertinimo proceso turinys (atliekama dokumentų turinio analizė (angl. *Content analysis*)), formuluojama hipotezė.

Antrajame etape Taikant kokybinio tyrimo strategiją atliekama kokybinė sisteminė juridinių ir kitų viešai prieinamų pirminių duomenų (valstybės informacinių sistemų saugos nuostatų ir kitų kibernetinio saugumo valdymo dokumentų turinio (angl. *Content*)) analizė, formuluojamos informacinės sistemos kibernetinio saugumo vertinimo modelio teorinės prielaidos, atliekama atvejo analizę (angl. *Case study*), išgryninami pagrindiniai informacinės sistemos kibernetinio saugumo vertinimo proceso elementai, identifikuojama vertinimo imtis, sukuriamas pradinis teorinis informacinės sistemos kibernetinio saugumo vertinimo modelis, nustatomi kriterijai, pagal kuriuos bus tikrinama hipotezė ir sukurtas modelis. Atliekama ekspertinė iš dalies struktūrizuota apklausa. Gauti duomenys analizuojami naudojant kokybinio turinio (angl. *Content*) metodą.

Tyrimo antrajame etape, atliekant atvejo analizę (angl. *Case study*), ekspertų kokybinę apklausą, suplanuoti tyrimai (žr. 10 pav.), kurie teikia papildomą gilesnę informaciją apie informacinės sistemos kibernetinio saugumo vertinimo procesą, procese vykdomas veiklas, proceso, kaip reiškinio problematiką, neatitikties (angl. *noncompliance*) atsiradimo priežastys, identifikuojamos galimos gerinimo priemonės.

Trečiame etape Empirinio tyrimo metu gautų rezultatų pagrindu tikrinamas teorinis informacinės sistemos kibernetinio saugumo vertinimo modelis, patvirtinama arba paneigiama hipotezė, identifikuojami objektyvaus informacinės sistemos kibernetinio saugumo vertinimo elementai, nustatomos informacinės sistemos kibernetinio saugumo vertinimo veiklų ribos. Atsižvelgiant į empirinio tyrimo rezultatus tikslinamas informacinės sistemos kibernetinio saugumo vertinimo modelis, įvertinamos sukurto modelio taikymo praktikoje galimybes ir pateikiami siūlymai dėl objektyvaus informacinių sistemų kibernetinio saugumo vertinimo proceso atlikimo ir gerinimo priemonių, kurios leistų organizacijoms siekti atitikties kibernetinio saugumo reikalavimams visuose organizacijos kibernetinio saugumo valdymo lygmenyse.



10 pav. Tyrimų loginė seka ir jų dermė

Šaltinis: parengta šio darbo autorės

Kokybinis empirinis tyrimas (ekspertų apklausa) atliktas 2023 m. kovo 27 d. – balandžio 20 d. Tyrimas buvo atliekamas etapais, kiekvieno etapo eiga, etapo metu vykdomos veiklos ir kiekvienos veiklos tikslas (rezultatas) pateikiami 4 lentelėje.

4 lentelė Kokybinio tyrimo (ekspertų apklausos) eiga

Etapo Nr.	Etapo pavadinimas	Etapo veiklos	Etapo veiklos tikslas, rezultatas
1.	Empirinio tyrimo (ekspertų apklausos) tikslų, vertinimo kriterijų formulavimas	Paruošiami su tyrimu susiję dokumentai (tyrimo pristatymas respondentui, klausimynai, kvietimai dalyvauti tyrime)	Paruoštas tyrimo pristatymas respondentui, paruoši apklausos klausimynai ekspertams, paruošti kvietimai dalyvauti tyrime
2.	Ekspertų atranka	Ekspertams elektroniniu paštu išsiunčiami kvietimai dalyvauti tyrime	Gautas eksperto sutikimas dalyvauti tyrime
3.	Informacijos rinkimas	Su ekspertais susisiekiama elektroniniu paštu arba kitu, ekspertui priimtinu, būdu, išsiunčiami apklausos klausimynai arba paskiriamas susitikimas (naudojama Microsoft Teams platforma).	Gautas eksperto užpildytas klausimynas arba gauti atsakymai į klausimyną nuotolinio susitikimo metu (tokiu atveju su ekspertu pakartotinai susisiekiama persiunčiant klausimyną ir prašant eksperto patvirtinti, ar atsakymai surašyti teisingai).

4 lentelės tęsinys kitame puslapyje

4 lentelės tęsinys

4.	Informacijos analizė	Gauta informacija analizuojama, pašalinamos galimos klaidos (pvz. susisiekiama su respondentais siekiant įsitikinti kad jiems klausimynuose pateikta informacija yra aiški arba pasitikslinant dėl eksperto patirties, pateiktų atsakymų ir pan.)	Atlikta surinktos informacijos, būtinos informacinės sistemos kibernetinio saugumo vertinimo procesui, kaip reiškiniui, teoriniam pagrindimui įvertinti (klausimyno 1–3 klausimai), nustatyti vertinimo proceso imtį ir tobulintinas proceso ir (ar) atitikties kibernetinio saugumo reikalavimams sritis (klausimyno 4–8 klausimai)
5.	Rezultatų interpretavimas	Apibendrinama ekspertų atsakymuose pateikta nuomonė	Suformuluota bendra ekspertų nuomonė pateiktų klausimų ir atsakymų pagrindu
6.	Išvadų ir pasiūlymų pateikimas	Ruošiamos tyrimo išvados, struktūrizuojami pasiūlymai	Suformuluojamos tyrimo išvados, į kurias atsižvelgiama tikslinant informacinės sistemos vertinimo modelį, formuluojami pasiūlymai dėl informacinių sistemų kibernetinio saugumo vertinimo proceso gerinimo priemonių ir atitikties kibernetinio saugumo reikalavimams

Šaltinis: parengta šio darbo autorės

Tyrimo etika. Atliekant tyrimą vadovaujamasi šiais informatikos moksluose ir moksliniuose tyrimuose taikomais principais (Kalibatienė D., Simanavičienė R., 2021):

1. Savanoriško dalyvavimo – užtikrinamas laisvas ir savanoriškas respondentų dalyvavimas tyrime.

2. Informuoto asmens – užtikrinama prieiga prie visos su tyrimu susijusios informacijos.

3. Anonimiškumo ir neskelbtinos informacijos slaptumo užtikrinimo – moksliniame tyrime saugoma respondentų tapatybė ir užtikrinama, kad tyrėjas imsis visų įmanomų priemonių užtikrinančių duomenų konfidencialumą.

4. Pagarbos – respondentui apklausos metu pateikiama tik neutrali, objektyvi, orientuota į atliekamo tyrimo turinį informacija.

5. Teisingumo – respondentai tyrimui parenkami pagal konkrečius kriterijus, susijusius su magistrinio darbo tyrimo objektu (t.y. vertinant respondentų patirtį, atliekamas funkcijas ir pan.).

Tyrimo validumui užtikrinti taikomos tokios pagrįstumo gerinimo strategijos (Kalibatienė D., Simanavičienė R., 2021):

1. trianguliacija (angl. *triangulation*), kuri leidžia tyrėjui susidaryti nuoseklų, įvairiapusišką vaizdą ir surinktų duomenų pagrindu patvirtinti rezultatus, daryti pagrįstas išvadas. Tyrime buvo taikomi skirtingi duomenų rinkimo būdai:

1.1. iš dalies struktūruotos (angl. *semi-structured*) kokybinės apklausos būdu buvo apklausiami skirtingų organizacijų ekspertai, saugos įgaliotiniai, atsakingi už informacinių sistemų kibernetinio saugumo organizavimą asmenys ir NKSC ekspertai, teikiantys kibernetinio saugumo paslaugas;

1.2. dalyvių tikrinimas (angl. *member checking*), šis būdas leidžia patikrinti surinktų duomenų tikslumą. Dalyvių turimos ekspertinės patirties patikrinimas vyko surinkus duomenis (gavus užpildytus klausimynus), atliekant duomenų analizę. Be to buvo susisiekiama su respondentais siekiant įsitikinti kad jų pateikta informacija ir pastebėjimai yra tiksliai interpretuojami iš tyrėjo perspektyvos.

Tyrimo ribotumas. Šiame moksliniame darbe yra analizuojami tik su informacinių sistemų kibernetinio saugumo vertinimu susiję aspektai. Mokslinių straipsnių paieška buvo vykdoma pagal su tiriamu objektu tiesiogiai susijusius raktinius žodžius. Siekiant nustatyti optimalų mokslinių straipsnių informacinių sistemų kibernetinio saugumo tematika laikotarpį, šiame darbe daugiausia, t.y. 92 % buvo atliekama ne senesnių kaip 2018 m. mokslinių straipsnių analizė (žr. 5 lentelę).

5 lentelė Mokslinių straipsnių paieškai naudotų raktinių žodžių, straipsnių pavadinimų, jų publikavimo metų sąrašas

Eil. Nr.	Paieškos raktiniai žodžiai	Mokslinio straipsnio pavadinimas	Publikavimo metai
1.	„Cybersecurity" arba „Kibernetinis saugumas", „Kibernetinio saugumo"	Cybersecurity, our digital anchor: a European perspective	2020
		Italian National Framework for Cybersecurity and Data Protection	2020
		Kibernetinio saugumo valdymo gerinimas taikant atsparumo modelius organizacijose	2019
		Lietuva pasaulinio kibernetinio saugumo reitingo dešimtuke! Kas slepiasi po šiuo reitingu?	2021
		Lietuvos kibernetinio saugumo kompetencijų žemėlapis	2022
		The role of cyber security audits in managing company systems and applications	2020
2.	„Cybersecurity framework" arba „Framework for Cybersecurity" arba „Information security framework"	Design of Cybersecurity Risk Assessment Tool for Small and Medium Sized Businesses using the NIST Cybersecurity Framework	2018
		Italian National Framework for Cybersecurity and Data Protection	2020
		Cybersecurity framework selection: comparison of NIST and ISO 27001	2023
		Information Security Governance Frameworks in Cloud Computing an Overview	2018
3.	„Information system security" arba „Information system security assessment"	Information System Security: Human Aspects	2019
		Managing Information system Security and Policy	2006
		ISO 27001: Information Security Management Systems	2023
		Information Security in the National Security System in the Modern Age	2022
		Cyber Security Risk Modelling in Distributed Information Systems	2023
4.	„Cybersecurity Compliance" arba „Compliance and Cybersecurity" arba „Information security noncompliance"	Promoting Cybersecurity Compliance, Research Anthology on Privatizing and Securing Data	2021
		A Systematic Review of Cybersecurity Compliance Management	2022
		Convergence and divergence of regulatory compliance and cybersecurity, Issues in Information Systems	2021
		Factors impacting information security noncompliance when completing job tasks	2014
		Identifying factors of noncompliance, compliance with information security policy and behavior change to compliance	2022

5 lentelės tęsinys kitame puslapyje

5 lentelės tęsinys

5.	„Cybersecurity Assessment“ arba „Security Assessment“ arba Cyber Risk Assessment arba Rzikos vertinimas	Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies	2021
		A Review of Cyber-security Measuring and Assessment Methods for Modern Enterprises	2019
		A Review of Security Assessment Methodologies in Industrial Control Systems	2019
		IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors and risk ranking process	2020
		Informacinių technologijų rizikos vertinimo metodai ir tobulinimo sprendimai	2020

Šaltinis: parengta šio darbo autorės

Tyrimas buvo organizuojamas taip, kad ekspertams nebūtų sudarytos sąlygos atsakant į ekspertinio tyrimo metu pateiktus klausimus atskleisti informaciją, kuri pagal galiojančius teisės aktus (žr. LRĮ XI-1807, 2011, 43 straipsnio 1 ir 7 dalis) yra konfidenciali (pvz. informacija apie valstybės informaciniuose ištekliuose įdiegtas saugumo priemones ir (ar) valstybės informacinių išteklių pažeidžiamumą). Dėl šios priežasties ekspertų nebuvo prašoma įvardinti konkrečią valstybės informacinę sistemą, registrą ar tinklą, kurio atžvilgiu jis, vykdydamas saugos įgaliotinio ir (ar) atsakingo už informacinių sistemų kibernetinį saugumą asmens funkcijas, atlieka kasmetinius informacinių technologijų atitikties teisės aktuose nustatytiems kibernetinio saugumo reikalavimams vertinimus, rizikos vertinimus, dokumentų turinio vertinimus, technologinio pažeidžiamumo (angl. *Penetration testing*) ar socialinės inžinerijos (angl. *Social Engineering Penetration Test*) testavimus.

Tyrimo metu buvo analizuojamas ir vertinamas Lietuvos valstybės informacinių sistemų kibernetinis saugumas. Tyrimu buvo siekiama išnagrinėti procesą, kaip reiškinį, sukurti objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelį, kuris galėtų pakeisti ydingą neatitikties (formalios atitikties) praktiką Lietuvoje. Toks požiūris neleidžia daryti apibendrinimų ar išvadų apie visas informacines sistemas (pvz. vidaus administravimui skirtas ar kitų šalių informacines sistemas) ir apie neatitikties (angl. *noncompliance*) problemos mastą pasaulyje. Norint nagrinėti informacinių sistemų kibernetinio saugumo vertinimą ir atitikties kibernetinio saugumo reikalavimams problemos paplitimą kitose informacinėse sistemose ir (ar) kitose šalyse būtina nagrinėti šią temą toliau, atliekant tolimesnius mokslinius tyrimus.

3. INFORMACINĖS SISTEMOS KIBERNETINIO SAUGUMO VERTINIMO MODELIO FORMAVIMAS

3.1. Informacinės sistemos kibernetinio saugumo vertinimo modelio formavimo teorinės prielaidos

Pasauliniai informacijos saugumo valdymo, informacinių technologijų kibernetinio saugumo vertinimo analizės metodai galėtų būti realizuoti atliekant informacinių sistemų kibernetinio saugumo vertinimą. Tačiau jie nėra išvystyti Lietuvoje nacionaliniu lygmeniu. 2016-2022 m. Nacionalinėse kibernetinio saugumo būklės ataskaitose, 2022 m. Valstybinio audito ataskaitoje, 2021-2027 m. Visuomenės skaitmeninimo išankstinio poveikio vertinimo ataskaitoje, Lietuvos mokslininkų tyrimuose pažymima, kad nuo 2016 m. valstybės informacinių sistemų kibernetinis saugumas dažnai tik *de jure* atitinka Lietuvos teisės aktuose nustatytus kibernetinio saugumo reikalavimus. Organizacijos informacinių sistemų saugos dokumentuose formaliai apsibrėžia informacinių sistemų valdymui nustatytus kibernetinio saugumo reikalavimus bei šiems reikalavimams įgyvendinti taikomus procesus. Tačiau realus informacinių sistemų kibernetinio saugumo užtikrinimas neįgyvendinamas. Maža to, informacinių sistemų valdytojai ir (arba) tvarkytojai kibernetinio saugumo valdymo procedūrų nustatymą dažnai vertina kaip biurokratinę naštą. Dėl šios priežasties faktinis informacinės sistemos kibernetinis saugumas užtikrinamas ne sistemiškai, o *ad hoc* principu, t.y. kuomet nėra nustatytų aiškių atsakomybių, procesų ir jie nėra įgyvendinami kaip nuolatinė informacijos saugumo, kibernetinio saugumo valdymo sistema.

Įgyvendinant Lietuvos informacinių technologijų valdymo pertvarką iki 2026 m. Lietuvoje planuojama sukurti nacionalinę kibernetinio saugumo valdymo sistemą (toliau – nacionalinė KS valdymo sistema), Organizacinių ir techninių kibernetinio saugumo reikalavimų nacionalinės stebėsenos sistemos skaitmeninį sprendimą (toliau – KS reikalavimų stebėsenos sistema). Tačiau, kol nacionalinė KS valdymo sistema ir KS reikalavimų stebėsenos sistema nėra sukurtos, objektyviam informacinių sistemų kibernetinio saugumo vertinimui atlikti jau dabar reikalingas pasauliniais informacijos saugumo valdymo ir informacinių technologijų kibernetinio saugumo vertinimo metodais paremto modelio sukūrimas. Formuojant tokį modelį būtina identifikuoti pagrindinius informacinės sistemos kibernetinio saugumo vertinimo elementus, nustatyti vertinimo proceso imtį, t.y. veiklas ir priemones, kurios turi būti atliekamos ir (arba) vykdomos vertinimo metu.

Šiame darbe formuojant informacinės sistemos kibernetinio saugumo vertinimo modelį kompleksiškai yra atsižvelgiama į darbo teorinėje dalyje identifikuotą vertinimo proceso apimtį (detaliai aprašyta šio darbo 1.2 skyriuje), moksliniais tyrimais ir gerosios praktikos metodais pagrįstus informacinės sistemos kibernetinio saugumo valdymui užtikrinti būtinus kibernetinio saugumo vertinimo elementus. Todėl į formuojamą informacinės sistemos kibernetinio saugumo vertinimo

modelį yra įtraukiamos rizikos vertinimo, technologinio pažeidžiamumo testavimo (angl. *penetration testing*), darbuotojų atsparumo kibernetinėms grėsmėms testavimo (angl. s*ocial engineering penetration test*), saugos dokumentų turinio vertinimo veiklos ir šie informacinės sistemos kibernetinio saugumo valdymui užtikrinti būtini kibernetinio saugumo elementai:

1. Lietuvos nacionalinėje teisėje nustatyti RIS kibernetinio saugumo valdymo elementai, (aprašyti šio darbo 1.1 ir 1.3.5 skyriuose, nurodyti 3 priedo 8 lentelės 2 stulpelyje);

2. Minimalūs privalomi kibernetinio saugumo elementai pagal TIS 2 direktyvos 21 straipsnio 2 dalį (aprašyti šio darbo 1.1 skyriuje, nurodyti 3 priedo 8 lentelės 3 stulpelyje);

3. Gerosios praktikos metoduose nustatytos minimalios informacijos, kibernetinio saugumo valdymui taikomos organizacines ir technines priemones:

3.1. ISVS privalomi minimalūs informacijos saugumo valdymo elementai (aprašyti šio darbo 1.3.1 skyriuje, nurodyti 3 priedo 8 lentelės 4 stulpelyje);

3.2. NIST CSF organizacinių ir techninių priemonių kategorijos (aprašytos šio darbo 1.3.2 skyriuje, nurodytos 3 priedo 8 lentelės 5 stulpelyje).

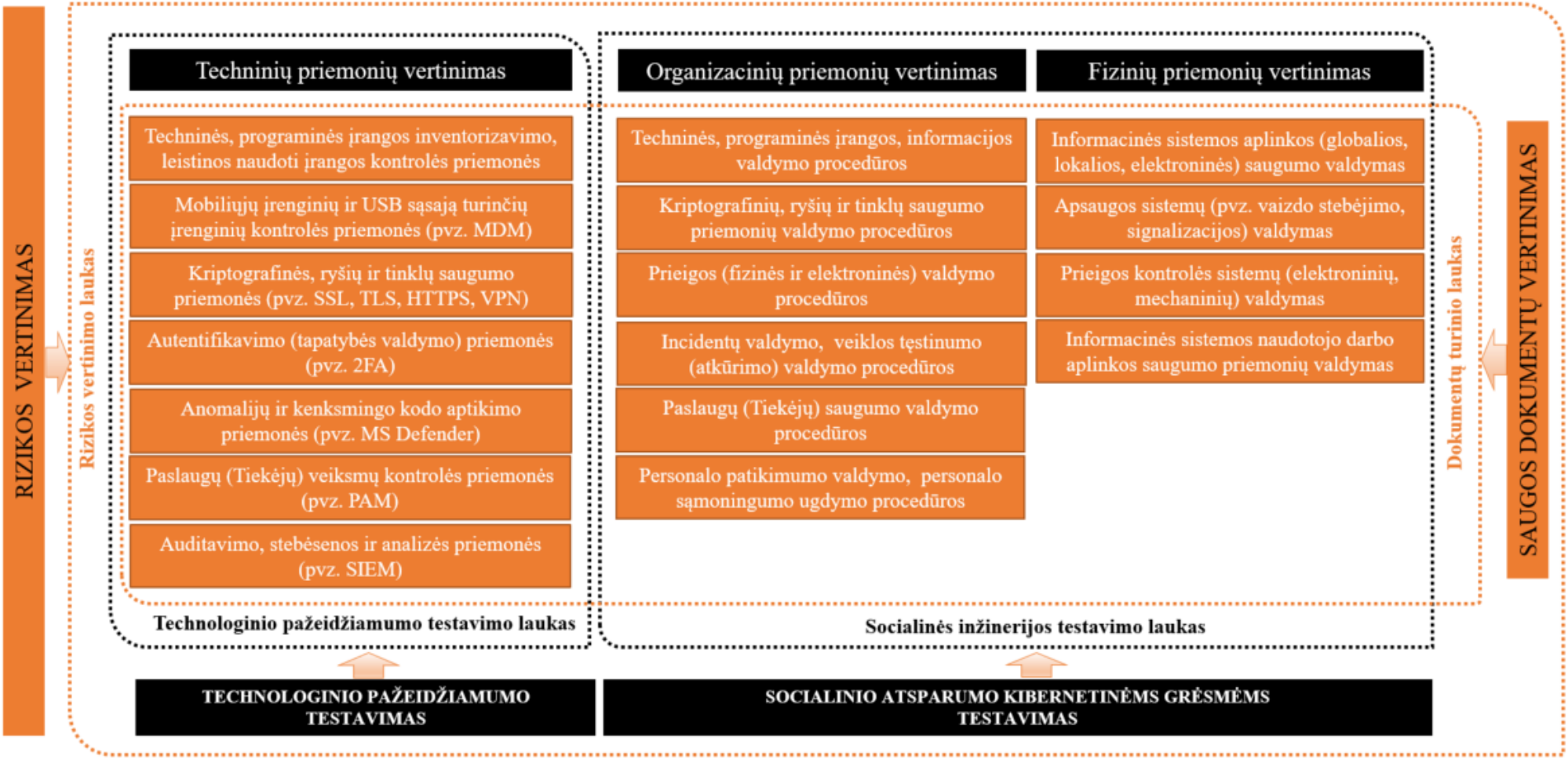
3.3. CIS Controls kibernetinei gynybai skirtos saugumo kontrolės priemonės (aprašytos šio darbo 1.3.3 skyriuje, nurodytos 3 priedo 8 lentelės 6 stulpelyje).

Kaip Europos Sąjungos ir Lietuvos nacionalinėje teisėje nustatyti ryšių (tinklų) ir informacinių kibernetinio saugumo valdymo elementai koreliuoja su gerosios praktikos metoduose nustatytais minimaliais reikalavimais informacijos, kibernetinio saugumo valdymui, kibernetinei gynybai taikomomis organizacinėmis ir techninėmis priemonėmis yra pademonstruota 4 priede pateiktoje 8 lentelėje Privalomų informacinių sistemų kibernetinio saugumo elementų, informacijos saugumo valdymo elementų, organizacinių ir techninių priemonių kategorijų bei kibernetinei gynyba skirtų kontrolės priemonių palyginimas.

Kuriant informacinės sistemos kibernetinio saugumo vertinimo modelį visi 4 priedo 8 lentelėje nurodyti privalomi informacinių sistemų kibernetinio saugumo elementai vadovaujantis gerosios praktikos metodais skirstomi į tokias tris kibernetinio saugumo valdymo kategorijas (detaliau aprašytos šio darbo 1.2 skyriuje):

1. Organizacinės valdymo priemonės;
2. Techninės valdymo priemonės;
3. Fizinės valdymo priemonės.

Pradinė informacinės sistemos kibernetinio saugumo vertinimo modelio struktūra pateikiama 11 pav. Teoriniai sukurto modelio pagrindai patikrinami atliekant empirinį tyrimą, analizuojant valstybės informacinių sistemų valdytojų ir (ar) tvarkytojų saugos įgaliotinių ir (ar) atsakingų už kibernetinio saugumo organizavimą ir (ar) kibernetinio saugumo paslaugas teikiančių ekspertų įžvalgas. Klausimai, į kuriuos buvo būtina atsakyti ekspertams pateikiami šio darbo 1 ir 2 prieduose.



11 pav. Informacinės sistemos kibernetinio saugumo vertinimo modelio struktūra

Šaltinis: parengta šio darbo autorės

3.2. Empirinio tyrimo ekspertų charakteristika ir apklausos klausimynų turinys

Kokybiniame tyrime dalyvavo 12 ekspertų:

1. 8 ne žemesnės kaip pirmos kategorijos ir (arba) ypatingos svarbos informacinių sistemų/registrų/tinklų valdytojų ir (ar) tvarkytojų paskirti saugos įgaliotiniai.
2. 2 atsakingi už informacinių sistemų kibernetinio saugumo organizavimą asmenys.
3. 2 NKSC ekspertai, kurių funkcijos susijusios su kibernetinio saugumo paslaugų teikimu.

Visi tyrime dalyvavę ekspertai yra valstybės institucijose ir (arba) valstybės įmonėse dirbantys specialistai. Dauguma (75 %) apklaustų ekspertų turi ne mažesnę kaip 10 m. patirtį vykdant saugos įgaliotinio ir (ar) atsakingo už informacinės sistemos kibernetinį saugumą asmens funkcijas, t.y. turi didelę patirtį organizuojant informacinių sistemų atitikties kibernetinio saugumo reikalavimams vertinimus, rizikos vertinimus, užtikrinant informacinių sistemų kibernetinį saugumą ir (arba) dirba kompetentingoje institucijoje, NKSC, padalinyje, kuris teikia kibernetinio saugumo paslaugas.

Visi ekspertai tyrime dalyvavo anonimiškai, jiems buvo priskirti unikalūs identifikavimo kodai. Detali informacija apie ekspertų patirtį, vykdomas funkcijas ir atsakymų į apklausos klausimynus pateikimo datas pateikiama 6 lentelėje.

6 lentelė Informacija apie ekspertų patirtį ir atsakymų į apklausos klausimynus pateikimo datas

Eksperto kodas	Eksperto patirtis (metais)	Eksperto vykdomos funkcijos	Apklausos gavimo data	Apklausos žodžiu atlikimo data
E_1	virš 3	Saugos įgaliotinis	2023-04-06	-
E_2	4	Saugos įgaliotinis	2023-04-11	-
E_3	20	Saugos įgaliotinis	2023-04-20	-
E_4	20	Saugos įgaliotinis	2023-03-30	-
E_5	10	Kibernetinio saugumo vadovas	-	2023-04-05
E_6	10	Saugos įgaliotinis	2023-04-05	-
E_7	18	Kibernetinio saugumo specialistas	2023-04-07	-
E_8	18	Saugos įgaliotinis	2023-04-17	-
E_9	17	Saugos įgaliotinis	2023-04-11	-
E_10	14	Saugos įgaliotinis	2023-04-04	-
E_N1	10	Kibernetinio saugumo paslaugų teikimas	2023-03-30	-
E_N2	7	Kibernetinio saugumo paslaugų teikimas	2023-04-06	-

Šaltinis: parengta šio darbo autorės

Ekspertams buvo pateikiami 8 (aštuoni) klausimai:

1. Valstybės informacinių sistemų valdytojų ir (ar) tvarkytojų saugos įgaliotiniams ir (ar) atsakingiems už informacinių sistemų kibernetinio saugumo organizavimą asmenims buvo pateikiami šio darbo 1 priede nurodyti klausimai.

2. NKSC kibernetinio saugumo paslaugas teikiantiems ekspertams buvo pateikiami šio darbo 2 priede nurodyti klausimai.

Tiek 1 tiek 2 priede pateikiamų klausimų turinys yra identiškas, tačiau, atsižvelgiant į tai, kad vieni ekspertai (pvz. saugos įgaliotiniai) atlieka informacinių sistemų vertinimo kibernetinio saugumo aspektu veiklas, o kiti ekspertai (pvz. NKSC specialistai) atlieka informacinių sistemų, jų saugos dokumentų atitikties kibernetinio saugumo reikalavimams veiklas, 2 klausimyne, siekiant užtikrinti tyrimo etikos principus, buvo pakeista 4 ir 6 klausimų formuluotė. Pavyzdžiui, klausimyno, skirto saugos įgaliotiniams ir (ar) atsakingiems už informacinių sistemų kibernetinio saugumo organizavimą asmenims, 4 klausime ekspertų buvo klausiama *„Kokias veiklas atliekate vertindami informacinių sistemų kibernetinį saugumą, informacinių technologijų atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams?“*, o klausimyne, skirtame NKSC ekspertui, teikiančiam kibernetinio saugumo paslaugas, 4 klausime buvo klausiama *„Jūsų nuomone, kokias veiklas reikėtų atlikti vertinant informacinės sistemos kibernetinį saugumą, informacinių technologijų atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams?*“. Taigi turinio prasme klausimai yra apie tą patį nagrinėjamą aspektą – informacinės sistemos kibernetinio saugumo vertinimo proceso metu vykdomų veiklų ir (ar) priemonių imties identifikavimą.

3.3. Ekspertinės apklausos duomenų analizė ir interpretacija.

Pateikiant iš dalies struktūrizuotos apklausos rezultatus, taikant kokybinio turinio (angl. *Content*) analizę, atsižvelgiant į klausimyno struktūrą ir ekspertų pateiktus atsakymus, išskiriamos tokios klausimų grupės:

1. Informacinės sistemos kibernetinio saugumo vertinimo proceso, kaip reiškinio, teorinis pagrindimas ir problematika.
2. Informacinės sistemos kibernetinio saugumo vertinimo proceso imties nustatymas.
3. Informacinės sistemos kibernetinio saugumo vertinimo proceso, atitikties kibernetinio saugumo reikalavimams vertinimo proceso tobulinimo kryptys.

Pirmoji klausimų grupė susijusi su darbo teorinėje dalyje atliktos mokslinių tyrimų, gerosios praktikos ir informacinių sistemų kibernetinį saugumą reglamentuojančių teisės aktų analizės pagrindu sukurto informacinės sistemos kibernetinio saugumo vertinimo modelio pagrindimu. Šiai siužetinei linijai priskirti šio darbo 1 ir 2 prieduose pateiktų klausimynų 1-3 klausimai, kuriais siekiama:

1. identifikuoti informacinių sistemų kibernetinio saugumo vertinimo proceso pagrindinius elementus (veiklas, kurios yra reikšmingos informacinės sistemos kibernetiniams saugumui užtikrinti);
2. identifikuoti gerosios praktikos metodų įtaką informacinės sistemos kibernetiniam saugumui;
3. identifikuoti formalios atitikties priežastis.

Su hipotezės, iškeltos šio darbo 1.3.5 skyriuje, patikrinimu yra susijęs 2 šios grupės klausimas.

Antroji klausimų grupė susijusi su informacinių sistemų kibernetinio saugumo vertinimo proceso praktiniais ypatumais, ekspertų patirtimi atliekant valstybės informacinių sistemų atitikties kibernetinio saugumo reikalavimams vertinimus. Šiai siužetinei linijai priskirti šio darbo 1 ir 2 prieduose pateiktų klausimynų 4-6 klausimai, kuriais siekiama:

1. identifikuoti kokias veiklas atlieka ekspertai ir (ar) kokias veiklas reikėtų atlikti vertinant informacines sistemas kibernetinio saugumo aspektu;

2. identifikuoti veiklas ir priemones, kurias reikėtų taikyti siekiant objektyviai įvertinti ar yra įgyvendinamos organizacijoje, informacinių sistemų saugos dokumentuose nustatytos organizacinės ir techninės kibernetinio saugumo priemonės;

3. identifikuoti metodus ir priemones, kuriuos taikant galima objektyviai atlikti informacinių sistemų rizikos vertinimus ir kibernetinio saugumo vertinimus.

Trečioji klausimų grupė susijusi su informacinių sistemų kibernetinio saugumo teisinio reglamentavimo trūkumais ir tobulintinomis kompetentingos institucijos (NKSC) teikiamomis kibernetinio saugumo paslaugomis. Šiai siužetinei linijai priskirti šio darbo 1 ir 2 prieduose pateiktų klausimynų 7-8 klausimai, kuriais siekiama:

1. identifikuoti kokios informacinių sistemų kibernetinio saugumo reglamentavimo sritys galėtų būti tobulinamos;

2. identifikuoti kokios NKSC teikiamos kibernetinio saugumo paslaugos informacinių sistemų kibernetinio saugumo vertinimo srityje galėtų būti tobulinamos.

Ekspertų apklausos kokybinio turinio analizė pateikiama 7 lentelėje.

7 lentelė Iš dalies struktūruotos ekspertinės apklausos kokybinio turinio (anlg. *Content*) analizė

1 KLAUSIMO TIKSLAS: ***identifikuoti pagrindines informacinės sistemos kibernetinio saugumo vertinimo proceso veiklas/priemones***		
Nr.	Veiklos/priemonės pavadinimas	Ekspertų teiginiai
1.1.	techninių priemonių diegimas ir naudojimas	E_1 <...***svarbi ir būtina*** kibernetiniam saugumui užtikrinti> E_2 <...***svarbi***> E_3 <...***reikšmingas*** kibernetiniam saugumui užtikrinti> E_4 <...***turi reikšmę*** IS saugos užtikrinimui> E_5 <...***turi didelę reikšmę***, IT, duomenų inventorizavimas-prioritetinis veiksmas> E_6 <...***svarbu*** ne tik kad veiktų, bet ir būtų nuolatiniai atnaujinimai ,,*up to date*“> E_7 <...***turi didelę reikšmę***, leidžia išvengti, atremti ir aptikti kibernetines atakas> E_8 <...***tai svarbiausios ir efektyviausios*** kibernetinio saugumo ***rizikų valdymo priemonės***> E_9 <...***turi didelę reikšmę***, <...> dar ***svarbiau, kad būtų taikoma kompleksiškai***, kartu su kitomis priemonėmis, nes tik tai duoda geriausią rezultatą> E_10 <...***didelę reikšmę***, užtikrina informacijos apdorojimo priemonių saugą> N_E1 <...***sustiprina*** IS kibernetinį saugumą <...> ***užtikrina*** IS apdorojamos ***informacijos vientisumą, konfidencialumą ir pasiekiamumą***> N_E2 <... ***svarbu*** užtikrinant kibernetinį saugumą ir atitiktį teisės aktams>
1.2	Organizacinių priemonių	E_1 <...***svarbi ir būtina*** kibernetiniam saugumui užtikrinti> E_2 <...***mažiau svarbi***>

7 lentelės tęsinys kitame puslapyje

7 lentelės tęsinys

	nustatymas ir taikymas	E_3 <...***reikšmingas*** kibernetiniam saugumui užtikrinti> E_4 <...***turi reikšmę*** IS saugos užtikrinimui> E_5 <...***labai svarbios***, ypač tęstinumo, incidentų valdymas > E_6 <...***labai svarbios***, kai nėra parašyta, neturi kuo vadovautis ir remtis. <...> Kontrolei ir išsireikalavimui reglamentavimas būtinas> E_7 <...***didelę reikšmę***> E_8 <...***nepakeičiama*** <...> ***organizuojant saugos procesus***> E_9 <...***turi didelę reikšmę***, <...> dar ***svarbiau, kad būtų taikoma kompleksiškai***, kartu su kitomis priemonėmis, nes tik tai duoda geriausią rezultatą> E_10 <...***labai svarbios***, nes žmonės valdo priemones, organizuoja procesus, labai svarbu, kad darbuotojai būtų aukštos kompetencijos, nes nuo žmonių priklauso, kaip bus valdoma sauga> N_E1 <...***sustiprina*** IS kibernetinį saugumą <...> ***užtikrina*** IS apdorojamos ***informacijos vientisumą, konfidencialumą ir pasiekiamumą***> N_E2 <...***svarbu*** užtikrinant kibernetinį saugumą ir atitiktį teisės aktams>
1.3.	fizinės aplinkos saugumui skirtų priemonių diegimas ir naudojimas	E_1 <...***svarbi ir būtina*** kibernetiniam saugumui užtikrinti> E_3 <...***reikšmingas*** kibernetiniam saugumui užtikrinti> E_2 <...***svarbi***> E_4 <...***turi reikšmę*** IS saugos užtikrinimui> E_5 <...priemonių svarba priklauso nuo organizacijos, jos ***turi būti proporcingos***> E_6 <...priklauso nuo organizacijos tipo ir veiklos. ***Labai svarbu, yra pagrindas***> E_7 <...***didelę reikšmę***> E_8 <...***aktualu rizikų valdymui, veiklos tęstinumo užtikrinimui***> E_9 <...***turi didelę reikšmę***, <...> dar ***svarbiau, kad būtų taikoma kompleksiškai***, kartu su kitomis priemonėmis, nes tik tai duoda geriausią rezultatą> E_10 <...***didelę reikšmę***> N_E1 <...***sustiprina*** IS kibernetinį saugumą <...> ***užtikrina*** IS apdorojamos ***informacijos vientisumą, konfidencialumą ir pasiekiamumą***> N_E2 <...***svarbu*** užtikrinant kibernetinį saugumą ir atitiktį teisės aktams>
1.4.	saugos nuostatų, kitų saugos politiką įgyvendinančių dokumentų kokybė, jų aktualumas ir atitiktis teisės aktuose nustatytiems reikalavimams	E_1 <...***svarbi ir būtina*** kibernetiniam saugumui užtikrinti> E_3 <...***reikšmingas*** kibernetiniam saugumui užtikrinti> E_2 <...***mažiau svarbi***> E_4 <...***turi reikšmę*** IS saugos užtikrinimui> E_5 <...***svarbi***, turi būti rengiami atsakingai ir peržiūrimi pagal poreikį> E_6 <...***labai svarbu***, kai nėra parašyta, neturi kuo vadovautis ir remtis. <...> Kontrolei ir išsireikalavimui reglamentavimas būtinas> E_7 <...***mažesnę reikšmę*** nei techninių priemonių naudojimas ir technologinio pažeidžiamumo testavimas <...> ***bet reikšminga***> E_8 <...***ypač svarbu kibernetinio saugumo rizikų vertinimui***> E_9 <...***turi didelę reikšmę***, <...> dar ***svarbiau, kad būtų taikoma kompleksiškai***, kartu su kitomis priemonėmis, nes tik tai duoda geriausią rezultatą> E_10 <...***dokumentai turi būti aiškūs***, ***suprantami ir iškomunikuoti suinteresuotoms šalims***, kad juos būtų galima įgyvendinti, laikytis nustatytų reikalavimų <...> ***aktualūs ir atitikti nustatytus reikalavimus***> N_E1 <...***sustiprina*** *IS kibernetinį saugumą* <...> ***užtikrina*** IS apdorojamos informacijos vientisumą, konfidencialumą ir pasiekiamumą> N_E2 <... ***svarbu*** užtikrinant kibernetinį saugumą ir atitiktį teisės aktams>
1.5.	technologinio pažeidžiamumo testavimų (*penetration testing*) atlikimas	E_1 <...***svarbi ir būtina*** kibernetiniam saugumui užtikrinti> E_2 <...***svarbi***> E_3 <...***reikšmingas*** kibernetiniam saugumui užtikrinti> E_4 <...***turi reikšmę*** IS saugos užtikrinimui> E_5 <...***be pasiruošimo*** atliekant ***gali sukelti tikrą incidentą***> E_6 <...***svarbu***, ***kad nebūtų tik „popierinis“ saugumas***> E_7 <..***didelę reikšmę***, suteikia galimybę sužinoti saugumo spragas, jas pataisyti>

7 lentelės tęsinys kitame puslapyje

7 lentelės tęsinys

		E_8 <...***ypač svarbu kibernetinio saugumo rizikų vertinimui***> E_9 <...***didelę reikšmę***, <...> dar ***svarbiau, kad būtų taikoma kompleksiškai***, kartu su kitomis priemonėmis, nes tik tai duoda geriausią rezultatą> E_10 <...***būtinas kiekvienai sistemai***, ***kuri pasiekiama iš išorės*** <...> turi būti atliekamas naujai kuriamoms ir esamoms sistemoms bent kartą per 3 metus, jei sistemoje pokyčių nėra, arba po kiekvieno reikšminio sistemos pokyčio> N_E1 <...***sustiprina*** IS kibernetinį saugumą <...> ***užtikrina*** IS apdorojamos informacijos vientisumą, konfidencialumą ir pasiekiamumą> N_E2 <... ***svarbu*** užtikrinant kibernetinį saugumą ir atitiktį teisės aktams>
1.6.	Darbuotojų, fizinės aplinkos atsparumo kibernetinėms grėsmėms testavimų atlikimas (pvz. soc. inžinerijos metodu)	E_1 <...***svarbi ir būtina*** kibernetiniam saugumui užtikrinti> E_2 <...***svarbi***> E_3 <...***reikšmingas*** kibernetiniam saugumui užtikrinti> E_4 <...***turi reikšmę*** IS saugos užtikrinimui> E_5 <...***darbuotojų mokymai–pagrindinė organizacinė priemonė***> E_6 <...***svarbiausias iš visų***. Nepadės dokumentai, techninė ir programinė įranga, jei darbuotojai aklai atidarinės laiškus, spaus ant nuorodų ir t.t. Nuolatinis mokymas turi būti> E_7 <...***didelę reikšmę***> E_8 <...***ypač svarbu kibernetinio saugumo rizikų vertinimui, žmogiškojo faktoriaus pažeidžiamumo testavimui***> E_9 <...***turi didelę reikšmę*** <...> dar ***svarbiau, kad būtų taikoma kompleksiškai***, kartu su kitomis priemonėmis, nes tik tai duoda geriausią rezultatą> E_10 <...***labai svarbus***, nes ***atskleidžia kibernetinio saugumo kultūrą organizacijoje***. <...> Testavimo rezultatai parodo spragas ir leidžia parinkti reikalingas mokymų, žinių ir įgūdžių stiprinimo priemones > N_E1 <...***sustiprina*** IS kibernetinį saugumą <...> ***užtikrina*** IS apdorojamos ***informacijos vientisumą, konfidencialumą ir pasiekiamumą***> N_E2 <...***svarbu*** užtikrinant kibernetinį saugumą ir atitiktį teisės aktams>
1.7.	rizikų vertinimas	E_1 <...***svarbi ir būtina*** kibernetiniam saugumui užtikrinti> E_2 <...***mažiau svarbi>*** E_3 <...***reikšmingas*** kibernetiniam saugumui užtikrinti> E_4 <...***turi reikšmę*** IS saugos užtikrinimui> E_5 <...***nuo rizikų vertinimo viskas turi prasidėti***> E_6 <...rizikų vertinimas yra ***pagrindas reikalingų priemonių*** (organizacinių ir techninių) ***pagrindimui*** vadovybei> E_7 <...***didelę reikšmę***> E_8 ***<...esminis procesas, nepalyginamai svarbesnis už atitikties vertinimą>*** E_9 <...***turi didelę reikšmę***, <...> dar ***svarbiau, kad būtų taikoma kompleksiškai***, kartu su kitomis priemonėmis, nes tik tai duoda geriausią rezultatą> E_10 <...***organizacija*** <...> ***turi identifikuoti ir valdyti visas su veikla susijusias rizikas***, ***jas prisiimti***, ***perduoti kitoms šalims*** arba ***parinkti kitus elgsenos su rizika būdus*** <...> kad grėsmės neišnaudotų pažeidžiamumų ir būtų išvengta žalos arba ji būtų minimali ir būtų užtikrintas organizacijos veiklos tęstinumas> N_E1 <...***sustiprina*** IS kibernetinį saugumą <...> ***užtikrina*** IS apdorojamos ***informacijos vientisumą, konfidencialumą ir pasiekiamumą***> N_E2 <...***svarbu*** užtikrinant kibernetinį saugumą ir atitiktį teisės aktams. ***Rizikos vertinimą iškeltume į pirmąją vietą*** >
2 KLAUSIMO TIKSLAS: *identifikuoti gerosios praktikos metodų įtaką informacinės sistemos kibernetiniam saugumui*		
Nr.	Veiklos/priemonės pavadinimas	Ekspertų teiginiai
2.	*Gerosios praktikos standartų (pvz.*	E_1 <...***Tai yra pagrindas***. <...> šios praktikos yra puikus darbų sąrašas ką reikia įgyvendinti> E_2 <...***taip***, nes ISO 27001 <...> reikalavimai skirti ISVS parengti>

7 lentelės tęsinys kitame puslapyje

7 lentelės tęsinys

	ISO/IEC 27001, NIST Cyber security framework, CIS Controls) metodų taikymas organizacijos veikloje ir jų įtaka IS kibernetiniam saugumui	E_3 <...***turi**, sertifikavimo auditų metu identifikuotų <...> trūkumų šalinimas stiprina tiek bendrą ISVS, tiek kibernetinį saugumą, kaip ISVS dalį*> E_4 <...***turi, tai** <...> **brandžios IS saugos gerinimo elementai***> E_5 <...***standartai prisideda prie** organizacijos ir informacinių sistemų **kibernetinio saugumo gerinimo**, ISO apima viską> E_6 <... ***labai naudinga turėti „karkasą“, kurio kryptimi einama**. ISO labiau skirta vadybai, o NIST ar CIS Controls – labiau techniniam saugumui užtikrinti. ISO 27001 <...> pagrindu vadovaujantis **lengviau įtraukti vadovybę ir kitus atsakingus asmenis** į saugumo procesą> E_7 <...***taip**. Pritaikius šių standartų reikalavimus pagerinamas informacinės sistemos kibernetinis saugumas> E_8 <... ***turi: susistemina požiūrį į kibernetinį saugumą** <...> tam kad panaudoti – reikia iki atitinkamo lygio subręsti*> E_9 <...***turi teigiamą įtaką, jei organizacija yra įsidiegusi** gerosios praktikos standartus **ir praktiškai (ne formaliai) juos taiko***> E_10 <...***labai prisideda prie kibernetinio saugumo stiprinimo**. **ISO 27001** plačiai naudojamas Lietuvoje, **privalomas organizacijoms, kurios tvarko I kategorijos informacines sistemas***> N_E1 <...***daro įtaką** <...> **gerosios praktikos standartai ir metodai reikalauja, kad būtų tinkamai įgyvendintos visos 1 klausime išvardintos priemonės***> N_E2 <...***gerosios praktikos yra gairės** organizacijoms **užtikrinant kibernetinį saugumą, pagalba parenkant saugos priemones** >
3 KLAUSIMO TIKSLAS:	***identifikuoti formalios atitikties priežastis***	
Nr.	Veiklos/priemonės pavadinimas	Ekspertų teiginiai
3.	*Formaliai apibrėžtų IS saugos dokumentų ir neatliekamų IS (IT) atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimų atsiradimo (egzistavimo) priežastys*	E_1 <...***dėl laiko stokos, finansavimo trūkumo**, arba **kai organizacija tiki kad pažįsta savo informacines sistemas***> E_2 <...***didelis darbų krūvis, finansavimo nebuvimas***> E_3 <...***žmogiškųjų išteklių trūkumas, finansavimo nepakankamumas, kompetencijos trūkumas***> E_4 <...***saugos personalo trūkumas** <..> **IS valdytojas nemato reikalo skirti resursų jo manymu nereikalingai veiklai***> E_5 <...***kiti prioritetai organizacijoje**, **organizacinėmis ir technologinėmis skolomis nenorima užsiimti, nes tai nesukuria pridėtinės vertės**, kol kas nors rimto nenutinka> E_6 <...1. ***formalus vadovybės požiūris**; 2. **neskiriama lėšų, dažnai saugumas tapatinamas tik su IT**; 3. **Specialistų, kompetencijų, trūkumas**. Sritis dinamiška, reikalauja nuolatinio mokymosi, IT ir vadybos žinių <...> **Neinvestuojama į žmones, jų mokymąsi, tobulėjimą***>. E_7 <...nežinau> E_8 <...***neveiklios kontrolės institucijos, pasenę reikalavimai, motyvacijos nebuvimas**, **dėl nežinojimo neapgalvotai suformuotas suvokimas ir praktika, privedę prie dabartinės situacijos**, *kai visiems patogu, kol nėra problemų.*> E_9 <...***žmogiškųjų resursų ir (ar) kompetencijų stoka***> E_10 <...***organizacijoms trūksta kibernetinio saugumo specialistų arba jie yra apkrauti**, todėl tinkamai nevykdomos su sauga susijusios veiklos> N_E1 <.***mažas vadovų dėmesys kibernetiniam saugumui, specialistų trūkumas***> N_E2 <...***žmogiškųjų ir finansinių išteklių trūkumas**. Taip pat **kompetencijų trūkumas bei vadovų požiūris***>
4 KLAUSIMO TIKSLAS:	***identifikuoti veiklas, kurias ekspertai atlieka vertindami informacines sistemas kibernetinio saugumo aspektu***	
Nr.	Veiklos/priemonės pavadinimas	**Ekspertų teiginiai**
4.1	techninių priemonių	E_1 <...***organizuojama ir vykdoma***>

7 lentelės tęsinys kitame puslapyje

7 lentelės tęsinys

	diegimas ir naudojimas	E_2 <...***vykdoma***> E_3 <...***vykdoma***> E_4 <...***atliekama nustatytu periodiškumu***>. E_5 <...***atliekamas visaapimantis auditas***> E_6 <...***atliekama kartą per 1-3 m.*** pagal valdomų informacinių išteklių svarbą> E_7 <...***atliekame***> E_8 <...***taip***> E_9 <...***atliekame***> E_10 <..***taip***> N_E1 <...***būtina priemonė***> N_E2 <...***svarbu kibernetinio saugumo vertinimui***>
4.2.	organizacinių priemonių nustatymas ir taikymas	E_1 <...***organizuojama ir vykdoma***> E_2 <...***rečiau vykdoma***> E_3 <...***vykdoma***> E_4 <...***atliekama nustatytu periodiškumu***>. E_5 <...***atliekamas visaapimantis auditas***> E_6 <...***atliekama kartą per 1-3 m.*** pagal valdomų informacinių išteklių svarbą> E_7 <...***atliekame***> E_8 <...***taip***> E_9 <...***atliekame***> E_10 <..***taip***> N_E1 <...***būtina priemonė***> N_E2 <...***svarbu kibernetinio saugumo vertinimui***>
4.3.	fizinės aplinkos saugumui skirtų priemonių diegimas ir naudojimas;	E_1 <...***organizuojama ir vykdoma***> E_2 <...***vykdoma***> E_3 <...***vykdoma***> E_4 <...***atliekama nustatytu periodiškumu***>. E_5 <...***atliekamas visaapimantis auditas***> E_6 <...***rečiau, bet atliekama***> E_7 <...***atliekame***> E_8 <...***taip***> E_9 <...***atliekame***> E_10 <..***taip***> N_E1 <...***būtina priemonė***> N_E2 <...***svarbu kibernetinio saugumo vertinimui***>
4.4.	saugos nuostatų ir (ar) kitų saugos politiką įgyvendinančių dokumentų kokybė, jų aktualumas ir atitiktis teisės aktuose nustatytiems reikalavimams	E_1 <...***organizuojama ir vykdoma***> E_2 <...***vykdoma***> E_3 <...***vykdoma***> E_4 <...***atliekama nustatytu periodiškumu***>. E_5 <...***atliekamas visaapimantis auditas***> E_6 <...***bent kartą per metus peržiūrima***> E_7 <...***atliekame***> E_8 <...***taip***> E_9 <...***atliekame***> E_10 <..***taip***> N_E1 <...***būtina priemonė***> N_E2 <...***svarbu kibernetinio saugumo vertinimui***>
4.5.	technologinio pažeidžiamumo testavimų (angl. *penetration testing*) atlikimas;	E_1 <...***organizuojama ir vykdoma***> E_2 <...***rečiau vykdoma***> E_3 <...***vykdoma***> E_4 <...***atliekama nustatytu periodiškumu***>. E_5 <...***atliekamas visaapimantis auditas***> E_6 <...***bent kartą per metus, priklauso nuo turimų finansinių išteklių. Geriausia, kai tai atlieka nešališki ir sertifikuoti išorės rangovai***>

7 lentelės tęsinys kitame puslapyje

7 lentelės tęsinys

		E_7 <...***atliekame***> E_8 <...***taip***> E_9 <...***atliekame***> E_10 <...***taip***> N_E1 <...***būtina priemonė***> N_E2 <...***svarbu kibernetinio saugumo vertinimui***>
4.6.	darbuotojų ir fizinės aplinkos atsparumo kibernetinėms grėsmėms testavimų atlikimas (pvz. socialinės inžinerijos metodu);	E_1 <...***organizuojama ir vykdoma***> E_2 <...***vykdoma***> E_3 <...***rečiau vykdoma***> E_4 <...***atliekama nustatytu periodiškumu***>. E_5 <...***atliekamas visaapimantis auditas***> E_6 <..***nuolat .. patiems atliekant*** <..> ***perkant paslaugą*** <..> dalyvaujant nacionalinėse kibernetinio saugumo pratybose, kurių pagalba testuojami veiklos tęstinumo planai, patikrinama ,,kaip veikia“ vidiniai, išoriniai teisės aktai> E_7 <...***atliekame***> E_8 <...***taip***> E_9 <...***atliekame***> E_10 <..***taip***> N_E1 <...***būtina priemonė***> N_E2 <...***svarbu*** kibernetinio saugumo vertinimui>
4.7	rizikų vertinimas	E_1 <...***organizuojama ir vykdoma***> E_2 <...***rečiau vykdoma***> E_3 <...***vykdoma***> E_4 <...***privalomai atliekama nustatytu periodiškumu***>. E_5 <...***atliekamas visaapimantis auditas***> E_6 <...***daroma kasmet ir įvykus neeiliniams pokyčiams***> E_7 <...***atliekame***> E_8 <...***taip***> E_9 <...***atliekame***> E_10 <..***taip***> N_E1 <...***būtina priemonė***> N_E2 <...***svarbu kibernetinio saugumo vertinimui***>
4.8	kitos veiklos	E_1 <...***tikėtinų incidentų sprendimų scenarijai***> E_3 <...***SOC*** *(Security Operation Centre) padalinio nuolatinė veikla žurnalinių įrašų (log files),* ***kibernetinių grėsmių ir incidentų stebėjimas***> E_4 <...***veiklos atstatymo plano patikra stalo pratybų metu, nors pageidautina, kad tokia patikra būtų reali***> E_7 <...***kibernetinio saugumo, veiklos tęstinumo pratybos***> E_8 <.***stebėsena, matavimai, trūkumų šalinimo ir priemonių vykdymo kontrolė***> E_9 <...***mokymai. Svarbu periodiškai šviesti darbuotojus ir kelti darbuotojų kibernetinio saugumo raštingumą***> N_E2 <...***labai svarbus veiklos tęstinumo valdymo užtikrinimas*** organizacijoje, <...> ***veiklos tęstinumo reguliarus išbandymas*** (testavimas)>
5 KLAUSIMO TIKSLAS: ***identifikuoti veiklas, priemones, kurias reikėtų taikyti siekiant objektyviai įvertinti ar yra įgyvendinamos organizacijoje, informacinių sistemų saugos dokumentuose nustatytos organizacinės ir techninės saugumo priemonės***		
Nr.	Veiklos/priemonės pavadinimas	Ekspertų teiginiai
5.	Veiklos, priemonės, kurias taikant organizacija gali objektyviai įvertinti, ar yra įgyvendinami IS	E_1 <...***skirti daugiau laiko ir žmogiškųjų išteklių***> E_2 <...***kasmet išoriniams auditoriams įvertinti IS saugą***> E_3 <...***ISO 27K sertifikavimas, NKSC patikra*** *organizacinių ir techninių kibernetinio saugumo reikalavimų atitikčiai,* ***išorės saugos audito paslaugos***> E_4 <...***nieko kito, tik nepriklausomas (trečios šalies) saugos auditas*** (visaapimantis, techninis, organizacinis, atitikties)>

7 lentelės tęsinys kitame puslapyje

7 lentelės tęsinys

	saugos dokumentuose nustatyti organizaciniai ir techniniai kibernetinio saugumo reikalavimai	E_5 <...***laikytis funkcijų atskyrimo principų, auditus turi atlikti dedikuoti asmenys, trečiosios šalys***> E_6 <...***atlikti atitikties, rizikos vertinimus, soc. inžinerijos testavimus, vykdyti mokymus, peržiūrėti teisės aktus; atlikti kasmetinius įsilaužimų testavimas (išorės) ir periodinius technologinių pažeidžiamumų vertinimas*** (patiems ir bent ***kartą per 3 m. išorės specialistų***). Esant galimybei, atlikti ugniasienių apkrovos testavimus, duomenų bazių konfigūracijų ir pažeidžiamumų patikrą> E_7 <...***patikrinti ar reikalavimai yra įgyvendinti***> E_8 <...***organizacijai samdytis nepriklausomus vertintojus***, *įsidiegti ISVS.* ***Kontroliuojančioms institucijoms – daryti saugos patikrinimus (auditus)***> E_9 <..*efektyviausia–****kibernetinio saugumo reikalavimų įgyvendinimo auditas***> E_10 <...***surinkti įrodymus ties kiekvienu reikalavimu***, siekiant nustatyti, ar jis yra tinkamai vykdomas ar įdiegtos kontrolės priemonės veikia. Reikalingas kiekvieno objekto patikrinimas ir įsitikinimas dėl reikalavimų įgyvendinimo. <...> ***Bent kartą per 3 metus pasitelkti išorės auditorius***> N_E1 <...***pasamdyti kompetentingus nepriklausomus ekspertus***> N_E2 <...***rizikos vertinimas padeda organizacijai valdyti kylančias rizikas***, parinkti technines, organizacines priemones nepriimtinoms rizikoms valdyti>
6 KLAUSIMO TIKSLAS: ***identifikuoti metodus ir priemones, kuriuos taikant galima objektyviai atlikti informacinių sistemų rizikos ir kibernetinio saugumo vertinimus***		
Nr.	Veiklos/priemonės pavadinimas	Ekspertų teiginiai
6.1.	Informacinių sistemų kibernetinio saugumo vertinimams atlikti naudojami metodai, priemonės	E_1 <...***naudojamos trečiųjų šalių paslaugos ir įsigyti įrankiai***> E_2 <...***išoriniai auditai***> E_3 <...*naudojame* ***ARSIS***> E_4 <...***periodiškai ir po didesnių pokyčių*** (technologinių ar saugos personalo) ***atliekamas saugos auditas***> E_5 <...***informacinių sistemų atitikties vertinimai integruoti į veiklos valdymo procesus***, taikome ARSIS metodiką kaip pagrindą> E_6 <...***LR teisės aktuose nustatytus reikalavimus***> E_7 <...***LR teisės aktuose nustatytus reikalavimus, ISO 27001 standarto,*** kitas gerąsias praktikas, technologinio pažeidžiamumo testavimas, ***atliekamas tiek automatizuotomis priemonėmis, tiek rankiniu būdu***, tikrinamas organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimas, matuojamas jų veiksmingumas> E_8 <...***remiamės teisės aktų nustatyta metodika***> E_9 <...mūsų įstaigoje ***sudaroma darbo grupė*** <...> ***siekiant vertinimus atlikti pilnavertiškai, yra svarbus skirtingų sričių specialistų įtraukimas***>. E_10 <...***IT saugos atitikties vertinimo metodika, pažeidžiamumų skenavimo priemonės, CMDB*** (Configuration Management DataBase), ***darbuotojų apklausa, įrodymų pateikimas*** (printscreen, įvykių žurnalai, patikra vietoje)> N_E1 <...***pasamdyti kompetentingus nepriklausomus ekspertus***> N_E2 <...***Vadovybės komunikacija apie kibernetinės saugos svarbą organizacijoje***. Reikalavimus apsibrėžti vidiniuose teisės aktuose <...> ***Paskirti atsakingus asmenis***. ***Vadovautis LR teisės aktais, tarptautiniais standartais ir gerosiomis praktikomis***>
6.2.	Rizikų vertinimams atlikti naudojami metodai, priemonės	E_1 <...***naudojamos trečiųjų šalių paslaugos ir įsigyti įrankiai***> E_2 ** E_3 <...*naudojame* ***ARSIS***> E_4 <...***periodiškai ir pagal poreikį atliekamas rizikos vertinimas***> E_5 <...***rizikos valdymo metodus. IS kibernetinio saugumo rizikos vertinimai integruoti į veiklos valdymo procesus***, taikome ARSIS metodiką kaip pagrindą> E_6 <...***Rizikos analizės vadovas, ISO 27005, kiekybinius, kokybinius metodus***> ** - ekspertas nepateikė atsakymo

7 lentelės tęsinys kitame puslapyje

7 lentelės tęsinys

		E_7 <... *LR* ***teisės aktuose nustatytus, ISO 27001 standarto reikalavimus, Rizikos analizės vadovą, kitas gerąsias praktikas***> E_8 <...*remiamės* ***teisės aktų nustatyta metodika, tobuliname ją savo jėgomis***> E_9 <...***atskira rizikų vertinimo metodika. Vertinimą atlieka darbo grupė***> E_10 <...***ARSIS metodika, ISO 27005 standartas***> N_E1 <...*galima pasinaudoti* ***ARSIS paslaugomis*** <...> *ir* ***kitomis metodikomis***> N_E2 <...***Vadovautis LR teisės aktais, gerosiomis praktikomis***>
7 KLAUSIMO TIKSLAS: ***identifikuoti tobulintinas informacinių sistemų kibernetinio saugumo teisinio reglamentavimo sritis***		
Nr.	Priemonės pavadinimas	Ekspertų teiginiai
7.	Informacinių sistemų kibernetinio saugumo vertinimo priemonės, rekomendacijos, kurių pasigendama Lietuvos nacionaliniuose teisės aktuose	E_1 <...***pasigendame konkretumo techniniais klausimais, visa informacija išskaidyta per skirtingus teisės aktus***> E_2 <... ***Norėtųsi, kad viskas būtų aiškiai išdėstyta viename dokumente***> E_3 <...***Nėra konsoliduotas*** <...> ***teisinis reguliavimas*** <...> ***reikalavimai nėra integralūs*** <...> *Dėl tapačių, skirtinguose teisės aktuose išdėstytų reikalavimų <...> kibernetinio saugumo subjektai, valdantys ir (ar) tvarkantys valstybės informacinius išteklius, patiria didesnę administracinę naštą>* E_4 <...***saugos įgaliotinio statuso, kaip savarankiško ir nepriklausomo saugos personalo, nustatymas turėtų būti įtvirtintas įstatymu***. *Šiuo metu įstatymas* pernelyg mažai apibrėžia saugos įgaliotinio funkcijas, jo statuso ir teisių praktiškai neapima, paliekant tai informacinės sistemos nuostatų/saugos nuostatų lygmeniui. Dėl šios priežasties saugos įgaliotinių veikla priklauso nuo informacinės sistemos valdytojo ir gali varijuoti labai plačiuose rėmuose>* *E_5 <...**pasigendu informacinių išteklių valdymo strategijos. Nera jokios koncepcijos**. Įstatymas* keičiamas fragmentiškai, bet bendros idėjos nėra. Neaiškus prioritetas- ar IT infrastruktūra ar duomenys, ką norime valdyti ir kaip>* *E_6 <... vieni teisės aktai prieštarauja kitiems,* ***nesutvarkytos sąvokos***. ***Pasigendu vadovybės atsakomybių*** <...> ***daug atsakomybių užkrauta saugos įgaliotiniams*** <...> ***be vadovybės palaikymo jis nelabai ką padarys*** <...> *Neaiški kibernetinio saugumo vadovo rolė <...> dabar vis dažniau kalbama apie saugumo operacijų centrus (SOC) vidinius, išorinius, kaip paslaugą, bet jų rolės nėra išgrynintos.* E_7 <...***manau, kad šiuo metu reikalavimų teisės aktuose yra pakankamai***> E_8 <...***vertinimo metodika seniai neatnaujinta***, *joje daug subjektyvumo ir galimybių manipuliuoti rezultatais <...>* ***ARSIS seniai nėra tobulinama*** *ir dėl reikalavimų ir vertinimo metodikos >* E_9 <...***labiausiai pasigendu rekomenduojamos programinės įrangos, skirtos kibernetiniam saugumui užtikrinti, sąrašo***> E_10 <***IT saugos atitikties vertinimo metodika, Rizikos analizės vadovas yra pasenę. Trūksta metodinių rekomendacijų dėl saugos vertinimų,*** *kaip rekomenduojama vertinti kiekvieną objektą, kokius įrodymus surinkti, kaip elgtis, kai reikalavimai netaikomi arba įgyvendinamos kitokios saugos priemonės, kurios gali būti analogiškos arba lygiavertės <...>* ***trūksta standartinių pirkimo sąlygų reikalavimų dėl saugos vertinimų paslaugų pirkimo***. <...> ***NKSC/KAM galėtų parengti standartines saugos patikrinimo paslaugų pirkimo sąlygas (pasidalinti gerąja praktika)*** <...> *kad visos organizacijos vienodai suprastų reikalavimus paslaugoms ir paslaugų apimčiai. Tokiu būdu galėtų būti pakeltas kibernetinis saugos lygis ir kibernetinė kultūra Lietuvoje>* N_E1 <...***Nemažai visko yra teisės aktuose, visko nenumatysi*** <...> Internetinėje erdvėje <...> mokymo įstaigose yra informacijos, rekomendacijų, mokymų <...> ***visada galima pasiteirauti atsakingų institucijų***> N_E2 <...***Dažnesnis teisės aktų keitimas (tobulinimas) papildant kibernetinės saugumo priemonėmis***> * – Valstybės informacinių išteklių įstatymas

7 lentelės tęsinys kitame puslapyje

7 lentelės tęsinys

8 KLAUSIMO TIKSLAS: *identifikuoti tobulintinas kompetentingos institucijos (NKSC) teikiamas kibernetinio saugumo paslaugas*		
Nr.	Paslaugos pavadinimas	Ekspertų teiginiai
8.1.	informacinių sistemų saugos dokumentų projektų derinimo procesas	E_1** E_2 <...***tobulintinas***> E_3 ** E_4 <...***paslauga reikalauja iš NKSC didelių žmogiškųjų išteklių***> E_5 <...*sunku pakomentuoti ką tobulinti*> E_6 <...*pastabos pateikiamos pakankamai greitai*> E_7 <...*manau, kad atliekamas gerai*> E_8 <...***saugos dokumentų kaip unikalių kiekvienai informacinei sistemai rengimas yra perteklinis***> E_9 <...*paprastai vyksta sklandžiai*> E_10 <.***galėtų būti parengti saugos dokumentų šablonai visoms organizacijoms***> N_E1 <...*planuojama automatizuoti ir tobulinti <...> kad vienoje platformoje būtų visiems prieinamų daug el. paslaugų, įrankių*> N_E1 <...*atsižvelgiant į stebėjimo rezultatus, nutarimus ir teisės aktus, atakų tendencijas NKSC kasmet tobulina savo teikiamas funkcijas*> ** - ekspertas nepateikė atsakymo
8.2.	informacinių sistemų techniniai kibernetinio saugumo būklės patikrinimai (*penetration testing*)	E_1 <...***būtų neįkainojama, jeigu NKSC galėtų atlikinėti penetration testus***> E_2 <...***tobulintinas***> E_3 <...***tobulintinas***> E_4 <...***galėtų būti NKSC teikiama paslauga tiek YSII tiek įslaptintos informacijos ir ryšių informacinėse sistemose***> E_5 <...*ne visomis NKSC paslaugomis naudojamės* > E_6 <...*NKSC resursų klausimas, bet* ***periodiškai, jei būtų atliekamas „netikėtas“ testavimas iš NKSC pusės – manau atneštų daugiau naudos****. Kai tai padarys įstaiga prie Krašto apsaugos ministerijos, tai atkreips vadovų dėmesį*> E_7 <...*atliekamas gerai*> E_8 <...***yra reikalavimas atlikti pažeidžiamumų vertinimą, tačiau jokios metodikos kaip jis turėtų būti atliekamas, kokie reikalavimai šiam vertinimui*** *ir svarbiausia –* ***nėra reikalavimų nustatytų pažeidžiamumų šalinimui***> E_9 <...***NKSC turėtų didinti tiek technologinius, tiek žmogiškuosius pajėgumus*** <...> ***organizacijos pačios turėtų rūpintis kibernetiniu saugumu***> E_10 <...***būtų naudinga, jeigu organizacijos galėtų iš NKSC užsakyti auditus***> N_E1 <...***planuojama automatizuoti ir tobulinti*** <...> kad vienoje platformoje būtų visiems prieinamų daug el. paslaugų, įrankių> N_E2 <...atsižvelgiant į stebėjimo rezultatus, nutarimus ir teisės aktus, atakų tendencijas ***NKSC kasmet tobulina savo teikiamas funkcijas***>
8.3.	organizacinių ir techninių kibernetinio saugumo reikalavimų stebėsena.	E_1** E_2** E_4 <...*paslauga reikalauja iš NKSC didelių žmogiškųjų išteklių,* ***reikalavimų stebėsena ARSIS pagalba yra formali***> E_5 <...***ne visomis NKSC paslaugomis naudojamės***> E_6 <...***periodiniai auditai – nepakenktų****, po jų – dažni teigiami pokyčiai ir žmogiškųjų išteklių srityje ir techninių sprendimų įsigijime.*> E_7 <... manau, kad ***atliekamas gerai***> E_8 <***NKSC turi galimybes stebėsenai (ARSIS) tačiau tuo efektyviai neužsiima***> E_9 <...*vien stebėti nepakanka.* ***Institucijoms būtina stiprinti ir didinti savo kibernetinės saugos pajėgumus***> ** – ekspertas nepateikė atsakymo

7 lentelės tęsinys kitame puslapyje

7 lentelės tęsinys

		E_10 <...***tikslinga tobulinti ARSIS***, *kad į ją būtų galima kuo paprasčiau pateikti duomenis <...> optimizuoti procesą, pvz., IS valdytojams ataskaitas teikti per ARSIS, joje suteikti galimybę susipažinti, kad tvarkytojams nereikėtų siųsti ataskaitų atskira*i> N_E1 <... ***planuojama automatizuoti ir tobulinti*** <...> *kad vienoje platformoje būtų visiems prieinamų daug el. paslaugų, įrankių*> N_E2 <...*atsižvelgiant į stebėjimo rezultatus, nutarimus ir teisės aktus, atakų tendencijas* ***NKSC kasmet tobulina savo teikiamas funkcijas***>

3.4. Empirinio tyrimo apibendrinti rezultatai.

Empirinio tyrimo rezultatai parodė, kad visi šio darbo teorinėje dalyje identifikuoti informacinės sistemos kibernetinio saugumo vertinimo proceso elementai, pagrįsti moksliniais tyrimais ir gerosios praktikos metodais, yra svarbūs ir turi reikšmę informacinės sistemos kibernetiniam saugumui užtikrinti.

Absoliučiai visi (100 %) tyrime dalyvavę ekspertai patvirtino, kad gerosios praktikos metodai turi įtaką informacinės sistemos kibernetiniam saugumui. Ekspertai pažymėjo, kad gerosios praktikos pagrindu į organizacijos kibernetinio saugumo valdymo procesą įtraukiama vadovybė, kiti organizacijos atsakingi asmenys, formuojamas sisteminis požiūris ne tik į informacinės sistemos kibernetinį saugumą, bet ir į visos organizacijos kibernetinio saugumo valdymą, informacijos saugumo procesų gerinimą, efektyvumą. Ekspertai pažymėjo, kad gerosios praktikos taikymas – tai brandaus požiūrio į informacinės sistemos saugos gerinimą indikatorius. Ekspertų nuomone labai svarbu, kad atitiktis gerosios praktikos standartui organizacijoje būtų objektyvi, ne deklaruojama. Tokiu būdu ekspertų pateikta nuomonė patvirtina įžvalgas, suformuluotas šio darbo teorinėje dalyje (žr. 1.3.5 skyrių), kad pirmos kategorijos informacinių sistemų valdytojų ir (ar) tvarkytojų ekspertų požiūris į tarptautinių standartų taikymą organizacijos veikloje ir jų įtaka informacinės sistemos kibernetiniam saugumui turėtų būti teigiamas. Atsižvelgiant į ekspertų nuomonę galima teigti, kad šio darbo teorinėje dalyje iškelta hipotezė, kad gerosios praktikos metodai turi teigiamą įtaką informacinės sistemos kibernetiniam saugumui ir visos organizacijos kibernetiniam saugumui, yra patvirtinta.

Identifikuojant pagrindines neatitikties kibernetinio saugumo reikalavimams priežastis, ekspertai išskyrė tokias pagrindines, tarpusavyje susijusias, formalios atitikties atsiradimo aplinkybes:

1. Kompetentingų informacijos saugos ir kibernetinio saugumo specialistų trūkumas;
2. Nepakankamas, formalus informacinės sistemos valdytojo ir (ar) tvarkytojo vadovų požiūris į informacijos/informacinės sistemos saugą, kuris pasireiškia tokiais veiksniais:

2.1. Neinvestuojama į atsakingų už informacijos/kibernetinį saugumą specialistų kompetencijų ugdymą, darbuotojų kibernetinio sąmoningumo mokymus, organizacines ir technines saugumo priemones (klaidingai manoma, kad investicijos į šias priemones nesukuria organizacijai pridėtinės vertės, pelno);

2.2. Atsakingų už informacijos/kibernetinį saugumą specialistų apkrova vykdomomis rolėmis, atsakomybėmis ir funkcijomis („žmogaus – orkestro“ fenomenas);

3. Kontrolės institucijų neveiklumas dėl žmogiškųjų ir techninių resursų stokos;

4. Pasenęs teisinis reglamentavimas.

Identifikuojant veiklas, kurias būtina atlikti vertinant informacines sistemas kibernetinio saugumo aspektu, 93 % ekspertų pažymėjo, kad informacinės sistemos kibernetiniam saugumui įvertinti būtina atlikti tokias veiklas: įdiegtų techninių priemonių vertinimą, nustatytų organizacinių priemonių vertinimą, fizinės aplinkos saugumo vertinimą, saugos nuostatų ir kitų saugos politiką įgyvendinančių dokumentų aktualumo ir atitikties teisės aktuose nustatytiems reikalavimams vertinimą, technologinio pažeidžiamumo testavimų (angl. *penetration testing*) vertinimą, darbuotojų ir fizinės aplinkos atsparumo kibernetinėms grėsmėms testavimų (pvz. soc. inžinerijos metodu) vertinimą, rizikų vertinimą. Ekspertai taip pat pažymėjo tokių papildomų priemonių kaip incidentų imitavimo scenarijaus, veiklos tęstinumo plano patikrinimų stalo pratybų metu ar kitų mokymų metu bei nuolatinės kibernetinių grėsmių, incidentų stebėsenos ir kontrolės svarbą.

Identifikuojant veiklas ir priemones, kurių taikymas yra būtinas siekiant objektyviai įvertinti ar yra įgyvendinamos organizacijoje, informacinių sistemų saugos dokumentuose nustatytos organizacinės ir techninės saugumo priemonės 75 % ekspertų pažymėjo išorės auditų svarbą – „organizacijoms tikslinga samdyti nepriklausomus vertintojus ar auditorius <...> kontroliuojančioms institucijoms (NKSC) – daryti saugos patikrinimus (auditus)“ organizacijų atžvilgiu.

Identifikuojant metodus ir priemones, kurių taikymas yra būtinas objektyviam informacinės sistemos atitikties kibernetinio saugumo vertinimui atlikti, dauguma ekspertų (80 %) pažymėjo išorės auditų bei kompleksinio, visaapimančio vertinimo, t.y. kai į vertinimo procesą įtraukiami skirtingų sričių specialistai (pvz. sudarant darbo grupes, pasitelkiant išorės ekspertus), taikomos gerosios praktikos metodai, skirtingos, viena kitą papildančios priemonės: organizacinės (pvz. apklausos, mokymai), techninės (pvz. pažeidžiamumų vertinimo), fizinės (pvz. darbuotojų veiklos ir (ar) aplinkos saugumo patikrinimas vietoje) svarba.

Identifikuojant metodus ir priemones, kurių taikymas yra būtinas objektyviam informacinės sistemos rizikų vertinimui atlikti, dauguma (70 %) ekspertų pažymėjo gerosios praktikos metodų (pvz. ISO 27001, ISO 27005, ARSIS) taikymo bei informacinių sistemų rizikų vertinimo proceso integravimo į organizacijos veiklos rizikos vertinimo procesus svarbą.

Identifikuojant kokios informacinių sistemų kibernetinio saugumo reglamentavimo sritys galėtų būti tobulinamos, dauguma (83 %) ekspertų pažymėjo, kad Lietuvos teisinis reglamentavimas turėtų būti tobulinamas. Ekspertų nuomone labiausia trūksta:

1. Holistinio požiūrio į informacinių išteklių valdymo teisinį reglamentavimą, t.y. kad viename dokumente, pvz., įstatyme, būtų:

1.1. aiškiai nustatytos sąvokos;

1.2. nustatyta informacinės sistemos valdytojo ir (ar) tvarkytojo vadovo atsakomybė;

1.3. nustatytos saugos įgaliotinio, kaip savarankiško ir nepriklausomo specialisto, teisės, pareigos ir funkcijos;

1.4. nustatyti organizaciniai ir techniniai kibernetinio saugumo reikalavimai.

2. Kompetentingos institucijos (pvz. NKSC) galėtų parengti metodines rekomendacijas dėl:

2.1. kibernetinės saugos vertinimų ir pažeidžiamumų vertinimo atlikimo;

2.2. standartinių sąlygų kibernetinės saugos vertinimo, technologinio patikrinimo paslaugų įsigijimo;

2.3. rekomenduojamos naudoti techninės ir (ar) programinės įrangos.

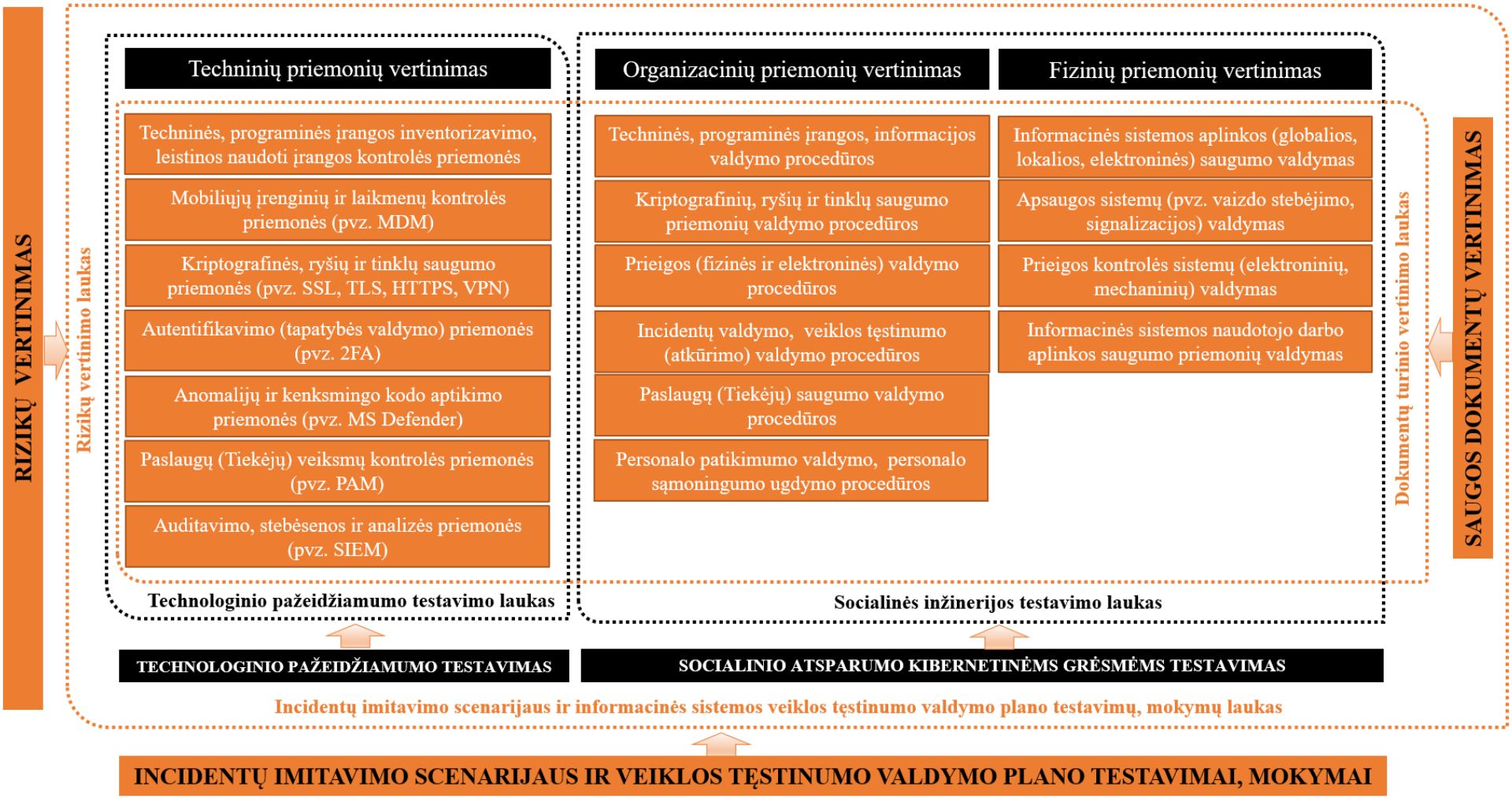
Identifikuojant tobulintinas kompetentingos institucijos (NKSC) teikiamų kibernetinio saugumo paslaugų informacinių sistemų kibernetinio saugumo vertinimo srityje veiklas, dauguma (70 %) ekspertų nurodė, kad labiausiai tikisi iš NKSC techninių kibernetinio saugumo būklės patikrinimų (angl. *penetration testing*) ir kitų auditų atlikimo. Ekspertų nuomone NKSC būtina plėsti savo technologinius, žmogiškuosius pajėgumus, ypač teikiant kibernetinio saugumo būklės patikrinimų paslaugas. Ekspertai taip pat pažymėjo, kad organizacijos privalo pačios rūpintis savo informacinių sistemų kibernetiniu saugumu, nelaukdamos incidento ar NKSC teikiamos pagalbos.

3.5.Patikslintas informacinės sistemos kibernetinio saugumo vertinimo modelis

Atlikus ekspertų apklausą nustatyta, kad visi teorinio informacinės sistemos kibernetinio saugumo vertinimo modelio pagrindiniai elementai yra būtini (privalomi) siekiant organizacijai atlikti objektyvų informacinės sistemos kibernetinio saugumo vertinimą. Ekspertai pasiūlė prie privalomų priemonių papildomai priskirti tokias priemones kaip incidentų imitavimo scenarijaus, veiklos tęstinumo plano testavimus ir mokymus (pvz. stalo pratybų metu). Šiomis veiklomis tikslinga papildyti kuriamą objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelį (žr. 12 pav.).

Ekspertų nuomone Lietuvos teisės aktuose nustatytos informacinių sistemų kibernetinio saugumo ir rizikos vertinimą reglamentuojančios metodikos ir priemonės (pvz. Informacinių technologijų saugos atitikties vertinimo metodika, ARSIS) yra pasenusios, todėl yra būtina taikyti gerosios praktikos metodus (pvz. ISO 27001, 27005 ir kt.) ir kitus visaapimančius informacinės sistemos kibernetinio saugumo vertinimo veiklos modelius, kurie galėtų užtikrinti objektyvaus informacinių sistemų kibernetinio saugumo vertinimo procesą.

Vienas iš tokių modelių galėtų būti pagal gerosios praktikos metodus sukurtas, empirinio tyrimo metu patikrintas, pagal ekspertų apklausos rezultatus patikslintas objektyvaus informacinių sistemų kibernetinio saugumo modelis, pateikiamas šio darbo 12 paveiksle.



12 pav. Objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelis

Šaltinis: parengta šio darbo autorės

IŠVADOS IR PASIŪLYMAI

1. Mokslinės literatūros, tarptautinės gerosios praktikos, Europos Sąjungos ir Lietuvos teisės aktų analizės metu nustatyta, kad:

1.1. Informacinės sistemos kibernetinis saugumas – tai informacinės sistemos gebėjimas būti atspariai bet kokiam informacijos saugumo įvykiui, bet kokiai grėsmei, kuri gali kilti kibernetinėje erdvėje ir informacinės sistemos veikimo ribose. Informacinės sistemos kibernetinio saugumo užtikrinimas – tai procesas, kurio metu informacijos saugumas valdomas (užtikrinamas) viso informacinės sistemos gyvavimo ciklo metu (žr. 1 paveikslą).

1.2. Informacinės sistemos kibernetinio saugumo vertinimas – periodinis, sistemingas, pagrįstas visuotinai pripažintais informacijos saugumo (konfidencialumo, vientisumo, prieinamumo) valdymo metodais, apimantis įvairias mokslo disciplinas, įtraukiantis skirtingų kompetencijų specialistus, procesas. Visapusiškam informacinės sistemos kibernetinio saugumo vertinimui atlikti būtina užtikrinti kad vertinime dalyvautų kompetentingi specialistai, o vertinimas apimtų bent šias veiklas:

1.2.1. Rizikų vertinimą;

1.2.2. Informacinės sistemos saugumui užtikrinti taikomų valdymo priemonių (teisinių, organizacinių, techninių, fizinių) vertinimą;

1.2.3. Informacinės sistemos saugos dokumentų vertinimą;

1.2.4. Informacinės sistemos veiklos (funkcionavimo) aplinkos vertinimą;

1.2.5. Informacinės sistemos technologinio pažeidžiamumo patikrinimą;

1.2.6. Socialinės inžinerijos pažeidžiamumų testavimus.

1.3. Organizacijoms, siekiančioms turėti struktūrizuotą, dokumentuotą informacinių sistemų kibernetinio saugumo valdymo politiką, tarptautiniai standartai (NIST CSF, ISO/IEC 27001, CIS Controls) pasiūlo tiek reikalavimus tiek rekomendacijas kaip reikalavimus įgyvendinti praktikoje, siekiant atitikties teisės aktuose nustatytiems reikalavimams. Iš visų standartų tik ISO/IEC 27001 leidžia organizacijai atlikti sertifikavimo procesą, gauti tarptautiniu mastu pripažįstamą ISO 27001 sertifikatą.

2. Remiantis atlikta mokslinės literatūros, tarptautinės gerosios praktikos, Europos Sąjungos ir Lietuvos teisės aktų analize galima daryti išvadą, kad objektyviam informacinės sistemos kibernetinio saugumo vertinimui atlikti būtinas holistinis požiūris į kibernetinio saugumo vertinimo procesą. Organizacijai, siekiančiai objektyvaus informacinės sistemos kibernetinio saugumo vertinimo, atitikties teisės aktuose nustatytiems kibernetinio saugumo reikalavimams, būtina taikyti holistiniu požiūriu, šiuolaikinių mokslinių strategijų, gerosios praktikos metodų (pvz. NIST CSF, ISO/IEC 27001, CIS Controls) ir kokybinės ekspertų nuomonės pagrindu sukurtą objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelį (pateikiamas šio darbo 12 paveiksle).

3. Atlikus kokybinį tyrimą buvo patvirtinta hipotezė, kad gerosios praktikos metodai (pvz. NIST CSF, ISO/IEC 27001, CIS Controls) turi teigiamą įtaką informacinės sistemos kibernetiniam saugumui ir visos organizacijos kibernetiniam saugumui. Visi tyrime dalyvavę ekspertai (informacinių sistemų valdytojų, tvarkytojų, kompetentingos institucijos (NKSC) atstovai) patvirtino gerosios praktikos metodų naudą taikant juos praktikoje. Ekspertai pažymėjo, kad gerosios praktikos metodų taikymas – tai brandžios informacinės sistemos, organizacijos elementai. Tyrimo metu buvo nustatytos šios formalios atitikties kibernetinio saugumo reikalavimams atsiradimo priežastys:

3.1. Kompetentingų informacijos/kibernetinio saugumo specialistų trūkumas;

3.2. Formalus informacinių sistemų valdytojų ir (ar) tvarkytojų vadovų požiūris į informacinių sistemų saugumą, pasireiškiantis tokiais veiksniais:

3.2.1. saugai dedikuotų žmogiškųjų išteklių trūkumu – vienam informacijos/kibernetinio saugumo specialistui deleguojama daug funkcijų, rolių, atsakomybių, užduočių;

3.2.2. investicijų į informacijos/kibernetinio saugumo specialistų kompetencijų ugdymą, darbuotojų kibernetinio sąmoningumo mokymus, organizacines ir technines priemones stoka.

3.3. vangi kontrolės institucijų veikla;

3.4. pasenęs teisinis reglamentavimas.

Ekspertų nuomone efektyviausios priemonės objektyviam informacinės sistemos kibernetiniam saugumui įvertinti – išoriniai, nepriklausomi auditai, gerosios praktikos metodų taikymas.

4. Sukurto objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelio taikymas praktikoje gali pagerinti organizacijos kibernetinio saugumo būklę visuose kibernetinio saugumo valdymo lygmenyse. Aukštesnė organizacijų kibernetinio saugumo branda būtina siekiant keisti Lietuvoje egzistuojančią ydingą neatitikties (formalios atitikties) praktiką. Šiam tikslui pasiekti reikėtų tobulinti:

4.1. informacinių sistemų kibernetinio saugumo teisinį reglamentavimą;

4.2. kompetentingos institucijos (NKSC) teikiamas kibernetinio saugumo paslaugas.

Atsižvelgiant į tyrimo rezultatus teikiami tokie siūlymai:

1. Organizacijai, siekiančiai objektyvaus informacinės sistemos kibernetinio saugumo vertinimo, atitikties teisės aktuose nustatytiems kibernetinio saugumo reikalavimams, aukštesnės kibernetinio saugumo brandos visuose kibernetinio saugumo valdymo lygmenyse siūloma:

1.1. informacinių sistemų kibernetinio saugumo vertinimą atlikti taikant objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelį (žr. 12 paveikslą),

1.2. į vertinimo procesą įtraukti visus atsakingus specialistus, įskaitant išorės ekspertus;

1.3. taikant gerosios praktikos metodus (pvz. NIST CSF, ISO/IEC 27001, CIS Controls) kurti organizacijos poreikius ir veiklą atitinkančią informacijos/kibernetinio saugumo valdymo sistemą;

1.4. stiprinti atsakingų už informacijos/kibernetinį saugumą specialistų kompetencijas, investuoti į darbuotojų kibernetinio sąmoningumo ugdymą (mokymus), organizacines ir technines priemones;

1.5. užtikrinti kibernetinio saugumo specialistų vykdomų funkcijų atskyrimą, rolių paskirstymą, pvz. atsižvelgti į ENISA siūlomą kibernetinio saugumo specialistų rolių sąrašą (žr. 1 lentelę);

1.6. atliekant informacinės sistemos kibernetinio saugumo vertinimus – taikyti gerosios praktikos metodus arba jų pagrindu sukurtus, organizacijai pritaikytus, metodus.

2. Kompetentingai ir kontroliuojančiai institucijai (NKSC) siūloma:

2.1. inicijuoti pasenusių teisės aktų (pvz., informacinių technologijų atitikties vertinimo metodikos) pakeitimus, taikyti holistinį, konsoliduojantį požiūrį į teisinį reglamentavimą;

2.2. tobulinti ARSIS;

2.3. dalintis sukaupta gerąja patirtimi ir praktika, pvz. parengti rekomendacijas dėl:

2.3.1. techninių kibernetinio saugumo būklės patikrinimų (angl. *penetration testing*), informacinės sistemos kibernetinio saugumo vertinimų, pažeidžiamumų vertinimo atlikimo;

2.3.2. informacinių sistemų kibernetinio saugumo vertinimo paslaugų įsigijimo;

2.3.3. rekomenduojamos naudoti programinės įrangos;

2.3.4. plėsti savo technologinius ir žmogiškuosius pajėgumus, ypač teikiant kibernetinio saugumo būklės patikrinimų (angl. k. *penetration testing*) paslaugas.

LITERATŪROS SĄRAŠAS

1. Angelini M., Ciccotelli C., Italian National Framework for Cybersecurity and Data Protection, ENISA Annual Privacy Forum 2020, (2020), 1-17 p. Prieiga per internetą: https://www.researchgate.net/publication/344840172_Italian_National_Framework_for_Cybersecurity_and_Data_Protection
2. Al-hashimi, M., Othman, M., Sulaiman, H., & Zaidan, A. A. (2018). Information Security Governance Frameworks in Cloud Computing an Overview. Journal of Advanced Computer Science and Technology Research, 8(2), 67-81 p. Prieiga per internetą: https://www.sciencedirect.com/science/article/pii/S2543925122000924?via%3Dihub
3. Alshar M., Cyber security framework selection: comparision of NIST and ISO 27001, Computing Journal, (2023). 1-11 p. Prieiga per internetą: CYBER-SECURITY-FRAMEWORK-SELECTION-COMPARISION-OF-NIST-AND-ISO27001.pdf (researchgate.net)
4. Baldini B., Barrero J., Tirendi ir kt. Cybersecurity, our digital anchor: a European perspective, European Commission, Publications Office of the European Union, (2020), 1-132 p. Prieiga per internetą: https://op.europa.eu/en/publication-detail/-/publication/a5e2b2af-dab3-11ea-adf7-01aa75ed71a1/language-en
5. Balžentis A., Žalimaitė M., Ekspertinių vertinimų taikymas inovacijų plėtros veiksnių analizėje: Lietuvos inovatyvių įmonių vertinimas, (2011), Vadybos mokslas ir studijos - kaimo verslų ir jų infrastruktūros plėtrai, 2011, Nr. 3 (27), 23-31 p. Prieiga per internetą: http://etalpykla.lituanistikadb.lt/fedora/objects/LT-LDB-0001:J.04~2011~1367176753634/datastreams/DS.002.0.01.ARTIC/content
6. Barčkutė O., Informacinių sistemų analizė, Vilnius, (2008), Vilniaus universitetas.
7. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, (2013), Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.454399?jfwid=
8. Bukauskas L., Brilingaitė A., Juozapavičius A., Ikamas K., Lepaitė D., Mokslinis tyrimas Lietuvos kibernetinio saugumo kompetencijų žemėlapis, (2022), 1-160 p. Prieiga per internetą: https://cs.vu.lt/projects/P-REP-21-2/ataskaita.pdf;
9. CIS Critical Security Controls®, v8, Prieiga per internetą: https://www.cisecurity.org/controls;
10. Dzemydienė D., Naujikienė R., Informacinės sistemos. Duomenų struktūros ir valdymas. Vadovėlis, Lietuvos teisės universitetas, Vilnius, (2004), 1-264 p.,
11. Dzemydienė D., Naujikienė R., Dzindzalieta R. Elektroninių paslaugų įgyvendinimo sprendimai, Mykolo Romerio Universitetas, Vilnius, (2016), 1-442 p.
12. Ekonomikos gaivinimo ir atsparumo didinimo planas „Naujos kartos Lietuva“ (2021), 1-406 p. Prieiga per internetą: Ekonomikos gaivinimo ir atsparumo didinimo planas „Naujos kartos Lietuva“ (lrv.lt)
13. Elektroninių paslaugų kūrimo metodika, patvirtinta Lietuvos Respublikos susisiekimo ministro 2015 m. spalio 7 d. įsakymu Nr. 3-416(1.5 E). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/149e25a06d2e11e5b316b7e07d98304b/asr
14. ENISA, Cybersecurity Culture Guidelines: Behavioral Aspects of Cybersecurity, (2019) 1-34 p. Prieiga per internetą: Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity — ENISA (europa.eu).
15. ENISA European Cybersecurity Skills Framework Role Profiles.(2022), 1-27 p., Prieiga per internetą: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles.
16. Europos Sąjungos skaitmeninio dešimtmečio kibernetinio saugumo strategija (2020), 1-31 p. Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52020JC0018
17. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr.

910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva), (2022), 1-73 p., prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32022L2555&from=LT

18. Fathi S., Hikal N., A Review of Cyber-security Measuring and Assessment Methods for Modern Enterprises, International journal on informatics visualization, (2019), Mansoura University, Prieiga per internetą: https://www.researchgate.net/profile/Said-Fathi-2/publication/335105910_A_Review_of_Cyber-security_Measuring_and_Assessment_Methods_for_Modern_Enterprises/links/5e66094d92851c7ce05360a9/A-Review-of-Cyber-security-Measuring-and-Assessment-Methods-for-Modern-Enterprises.pdf?origin=publication_detail

19. Gaižauskaitė I., Valavičienė N., Socialinių tyrimų metodai: kokybinis interviu, Mykolo Romerio universitetas, (2016), 1-394 p.

20. Grinevičius R., Kibernetinio saugumo valdymo gerinimas taikant atsparumo modelius organizacijose, (2019), 224 p,Prieiga per internetą:https://vb.mruni.eu/object/elaba:36356059/36356059.pdf

21. Gartner. 7 Top Trends in cybersecurity for 2022. Prieiga per internetą: Gartner Top Security and Risk Trends in 2022

22. Harris M. A., Martin R., Promoting Cybersecurity Compliance, Research Anthology on Privatizing and Securing Data, Research Anthology on Privatizing and Securing Data, (2021), 54-71 p. Prieiga per internetą: https://www.researchgate.net/publication/351831519_Promoting_Cybersecurity_Compliance;

23. Harrel M.N., Factors impacting information security noncompliance when completing job tasks Southeaastern University, (2014), 1-170 p. Prieiga per internetą: https://core.ac.uk/download/pdf/51072525.pdf

24. Hassan A., Binti A., Latif A. Identifying Factors of Non-Compliance, Compliance with Information Security Policy, and Behavior Change to Compliance: Literature Review. Vol.49, No.12, (2022), Prieiga per internetą: http://jonuns.com/index.php/journal/index

25. Huges Ch., The 7 CIS controls you should implement first, (2021), Prieiga per internetą: https://www.csoonline.com/article/3438119/the-5-cis-controls-you-should-implement-first.html

26. Idrisov H., Information security in the National security system in the modern age, Journal Fiat Justisia, Volume 16 Number 4, (2022), 1-10 p. Prieiga per internetą: https://www.researchgate.net/publication/365499030_Information_Security_in_the_National_Security_System_in_the_Modern_Age

27. Informacinių technologijų saugos atitikties vertinimo metodika, (2020). Prieiga per internetą:https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/117a33f038cb11eb8c97e01ffe050e1c?jfwid=

28. ISO/IEC 27001 standarts, Prieiga per internetą: https://www.iso.org/isoiec-27001-information-security.html.

29. ISO/IEC 27002 standarts, Prieiga per internetą: ISO - ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls

30. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems – Requirements Prieiga per internetą: https://www.iso.org/standard/82875.html

31. Ypatingos svarbos informacinės infrastruktūros identifikavimo metodika, (2018). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f?jfwid

32. Jadhav K.D, The role of cyber security audits in managing company systems and applications (2020), Prieiga per internetą: (PDF) THE ROLE OF CYBER SECURITY AUDITS IN MANAGING COMPANY SYSTEMS AND APPLICATIONS (researchgate.net)

33. Jevsejev R., Informacinių technologijų rizikos vertinimo metodai ir tobulinimo sprendimai, Mokslas–Lietuvos ateitis, Nr. 12, (2020), 1-7 p., Prieiga per internetą: Information technology risk assessment methods and improvement solutions | Mokslas – Lietuvos ateitis / Science – Future of Lithuania (vilniustech.lt)

34. Junaid T.S, ISO 27001: Information security management systems, (2023), 1-5 p., Prieiga per internetą:https://www.researchgate.net/publication/367166657_ISO_27001_Information_Security_Management_Systems

35. Kalibatienė D., Simanavičienė R, Moksliniai tyrimai ir inovacijos informatikos moksluose, Vilniaus Gedimino technikos universitetas, (2021), 1-398 p.

36. Kandsamy K., Srinivas K. ir kt. IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors and risk ranking process, EURASIP Journal an Information Security, (2020). Prieiga per internetą: IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process | EURASIP Journal on Information Security | Full Text (springeropen.com)

37. Leger M.A, A Systematic Review of Cybersecurity Compliance Management, (2022), 1-35 p. Prieiga per internetą:https://www.researchgate.net/publication/366723803_A_Systematic_Review_of_Cybersecurity_Compliance_Management;

38. Lietuvos kibernetinio saugumo įstatymas (2014). Prieiga per internetą: XII-1428 Lietuvos Respublikos kibernetinio saugumo įstatymas (lrs.lt)

39. Lietuvos visuotinėje enciklopedija, Vilnius, Mokslo ir enciklopedijų leidimo institutas, VIII tomas, (2005), Prieiga per internetą: https://www.vle.lt/straipsnis/informacine-sistema/

40. Lietuvos valstybės informacinių išteklių įstatymas (2011), Prieiga per internetą: XI-1807 Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas (lrs.lt)

41. Marotta A., Madnick S., Convergence and divergence of regulatory compliance and cybersecurity, Issues in Information Systems, Journal Issues in Information Systems Volume 22, Issue 1, (2021), 10-50 p. Prieiga per internetą: https://www.iacis.org/iis/2021/1_iis_2021_10-50.pdf

42. Mikalauskienė A., Brazaitis Z., Informacinių sistemų sauga, Vilnius, Vilniaus universiteto leidykla, (2006).

43. Nacionalinė kibernetinio saugumo būklės ataskaita (2016), 1-50 p. Prieiga per internetą: https://kam.lt/wp-content/uploads/2022/02/nksc_metine_ataskaita_uz_2016.pdf

44. Nacionalinė kibernetinio saugumo būklės ataskaita (2017), 1-25 p. Prieiga per internetą: https://kam.lt/wp-content/uploads/2022/02/nksc_ataskaita_2017_lt.pdf

45. Nacionalinė kibernetinio saugumo būklės ataskaita (2018), 1-56 p. Prieiga per internetą: https://kam.lt/leidiniai/nacionaline-kibernetinio-saugumo-bukles-ataskaita-2018/

46. Nacionalinė kibernetinio saugumo būklės ataskaita, (2019), Prieiga per internetą: https://kam.lt/wp-content/uploads/2022/02/nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2019.pdf;

47. Nacionalinė kibernetinio saugumo būklės ataskaita, (2020), 1-47 p. Prieiga per internetą: https://kam.lt/wp-content/uploads/2022/02/nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2020.pdf

48. Nacionalinė kibernetinio saugumo būklės ataskaita (2021) 1-57 p. Prieiga per internetą: https://kam.lt/wp-content/uploads/2022/08/Nacionaline-kibernetinio-saugumo-ataskaita-2021.pdf

49. Nacionalinis kibernetinių incidentų valdymo planas, (2018). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f?jfwid

50. Nacionalinė kibernetinio saugumo strategija (2018), Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f?jfwid ;

51. NKSC teikiamų kibernetinio saugumo paslaugų (servisų) sąrašas, Prieiga per internetą: https://www.nksc.lt/paslaugos.html

52. NIST Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (2018), 1-55 p. Prieiga per internetą: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

53. Kissel R., Stine K., Security Considerations in the Suystem Development Life Cycle, NIST Special Publication 800-64 Revision 2, (2019), 1-68 p. Prieiga per internetą: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-64r2.pdf

54. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas (2018), Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f?jfwid

55. Ponemon Institute, IBM Security, Cost of a Data Breach Report 2022“ (2022), 1-59 p. Prieiga per internetą: https://www.ibm.com/downloads/cas/3R8N1DZJ

56. Palko D., Babenko T., Cyber Security Risk Modeling in Distributed Information Systems, (2023), 1-23, Journal Applied Sciences, Prieiga per internetą: https://www.researchgate.net/publication/368498469_Cyber_Security_Risk_Modeling_in_Distributed_Information_Systems

57. Parker D.B. Computer security management Reston Prentice Hall, (1981), 308 p.

58. Patašienė I., Zaukas G. Kregždytė R., Patašius M., Informacinės sistemos ir socialinių duomenų analizė, Kauno technologijos universitetas, (2015), 1-144 p. Prieiga per internet: https://ebooks-ktu-edu.skaitykla.mruni.eu/product/informacins-sistemos-ir-socialini-duomen-analiz

59. Pritaikytosios ir standartizuotosios duomenų apsaugos informacinės sistemos gyvavimo ciklo gairės, (2020), 1-16 p. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Pritaikytoji_ir_standartizuotoji_apsauga_IS_gyvavimo_cikle_2020-12.pdf

60. Qassim Q., Jamil N., Daud M., Patel A. A Review of Security Assessment Methodologies in Industrial Control Systems, Information and Computer Security, Vol. 27 No. 1, (2019), 47-61 p. Prieiga per internetą: https://doi.org/10.1108/ICS-04-2018-0048, https://www.researchgate.net/publication/327207455_A_Review_of_Security_Assessment_Methodologies_in_Industrial_Control_Systems.

61. Roshanaei M., Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies, Journal of Computer and Communications, (2021), Nr.8, 80-102 p. Prieiga per internetą: https://www.scirp.org/journal/paperinformation.aspx?paperid=111501.

62. Registrų ir valstybės informacinių sistemų registras, Prieiga per internetą: https://registrai.lt/login.

63. A SANS 2021 Survey: OT/ICS Cybersecurity, (2021), Prieiga per internetą: https://www.sans.org/white-papers/SANS-2021-Survey-OTICS-Cybersecurity/

64. SANS 2019 State of OT/ICS Cybersecurity Survey, (2019), 1-23 p. Prieiga per internetą: https://www.forescout.com/resources/2019-sans-state-of-ot-ics-cybersecurity-survey/.

65. Simanauskas L. Informacinės sistemos. Vadovėlis. Vilnius, Vilniaus universiteto leidykla, (2000), 1-290 p.

66. Shouran Z., Priyambodo T.K, Ashari A., Information System Security: Human Aspects, International Journal of Scientific & Technology Research, 8(03), (2019) 1-115 p., Prieiga per internetą :https://www.researchgate.net/publication/331859493_Information_System_Security_Human_Aspects#fullTextFileContent

67. Saugos dokumentų turinio gairių aprašas, (2013), prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.454399?jfwid

68. Štitilis D., Lietuva pasalio kibernetinio saugumo reitingo dešimtuke ! Kas slepiasi po šiuo reitingu? Mykolo Romerio Universitetas, (2021), Prieiga per internetą: Lietuva pasaulinio kibernetinio saugumo reitingo dešimtuke! Kas slepiasi po šiuo reitingu? - MRU (mruni.eu).

69. Štitilis D., Pakutinskas P., Dauparaitė L, Laurinaitis M., Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai, Kolektyvinė mokslo monografija, Vilnius, Mykolo Romerio Universitetas, (2011), 1-509 p.

70. Svarbiausia Lietuvos kibernetinio saugumo būklės statistika ir tendencijos, 2021 m.-2022 m. I ketv., (2022), 1-17 p. https://kam.lt/wp-content/uploads/2022/08/Cyber-santrauka_V.9.0-2021.pdf

71. Trček D. Managing Information system Security and Policy, Berlin, Heidelberg: Springer Verlang, (2006), 1-236 p.

72. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašas, (2020), Prieiga per internetą:https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/117a33f038cb11eb8c97e01ffe050e1c?jfwid=

73. Valstybinio audito ataskaita „Kibernetinis saugumo užtikrinimas“, (2022), 1-54 p. Prieiga per internetą: https://www.valstybeskontrole.lt/LT/Product/24128/kibernetinio-saugumo-uztikrinimas

74. Valstybės informacinių išteklių valdymo įstatymas, (2011), Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/TAR.85C510BA700A/asr

75. Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašas, (2013).Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/TAR.A97664A25AC6/asr

76. Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas, (2013). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.454399?jfwid=

77. Valstybės informacinių sistemų gyvavimo ciklo valdymo metodika, (2014). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/296c87d09e8e11e383c0832a9f635113/asr

78. Venkatesh V., Design of Cybersecurity Risk Assessment Tool for Small and Medium Sized Businesses using the NIST Cybersecurity Framework, Kennesaw State University, (2018). Prieiga per internetą: (PDF) Design of Cybersecurity Risk Assessment Tool for Small and Medium Sized Businesses using the NIST Cybersecurity Framework (researchgate.net)

79. 2021-2027 m. Visuomenės skaitmeninimo išankstinio poveikio vertinimo paslaugų ataskaita (2020), prieiga per internetą: 2021–2027 m. visuomenės skaitmeninimo išankstinio poveikio vertinimas | 2014-2020 Europos Sąjungos fondų investicijos Lietuvoje (esinvesticijos.lt)

80. Вострецова, Е.В. Основы информационной безопасности, Jekaterinburgas, (2019), Prieiga per internetą: https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf?ysclid=le9zi0cioh784697380.

81. World Economic Forum, The Global Risk Report, (2022), 1-117 p. Prieiga per internetą: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf.

ANOTACIJA

Parnarauskienė A. (2023) X informacinės sistemos vertinimas kibernetinio saugumo aspektu (magistro baigiamasis darbas). Vilnius Mykolo Romerio universitetas

Magistro baigiamajame darbe taikant holistinį požiūrį yra išanalizuotas informacinės sistemos vertinimo kibernetinio saugumo aspektu procesas, išgryninami pagrindiniai proceso elementai, identifikuojama vertinimo imtis (veiklos ir priemonės), vertinimo problematika, neatitikties (formalios atitikties) atsiradimo priežastys. Taikant visuminį požiūrį, šiuolaikinius mokslinius ir gerosios praktikos metodus, kuriamas objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelis ir patikrinamas empiriškai, atliekant ekspertinį kokybinį tyrimą. Pirmame skyriuje analizuojami informacinės sistemos kibernetinio saugumo vertinimo teoriniai aspektai, išgryninami teoriniai proceso elementai, imtis ir identifikuojama informacinės sistemos kibernetinio saugumo vertinimo, atitikties kibernetinio saugumo reikalavimams problematika, iškeliama hipotezė. Antrame skyriuje pateikiama tyrimo metodologija, identifikuojami empirinio tyrimo dalyviai, duomenų rinkimo šaltiniai, duomenų rinkimo metodai, kokybinio tyrimo duomenų patikimumo užtikrinimo būdai. Trečiame skyriuje apibendrinami ir susisteminami ekspertinio tyrimo metu gauti duomenys, patvirtinama arba atmetama hipotezė, daromos išvados, tikslinamas teoriniu pagrindu sukurtas ir empiriniu tyrimu pagrįstas objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelis, identifikuojamos informacinių sistemų kibernetinio saugumo vertinimo proceso tobulinimo kryptys, pateikiami siūlymai objektyviam informacinės sistemos kibernetinio saugumo vertinimui atlikti.

Pagrindiniai žodžiai: Informacinė sistema, Informacinės sistemos saugumo vertinimas, Kibernetinis saugumas, Kibernetinio saugumo vertinimas, Atitiktis.

ANNOTATION

Parnarauskienė A. (2023) Assessment of X Information System at Cyber Security Aspects (master thesis). Vilnius: Mykolas Romeris University

In the master's thesis, applying a holistic approach, the process of information system assessment from the aspect of cyber security is analysed, the main elements of the process are refined, the assessment sample (activities and tools), assessment issues, causes of non-compliance (formal compliance) are identified. Using a holistic approach, modern scientific and best practice methods, a objective assessment model of information system cyber security is developed and empirically verified by an expert qualitative study. The first chapter analyses the theoretical aspects of the information

system cyber security assessment, refines the theoretical elements of the process, identifies the problems of information system cyber security assessment, compliance with cyber security requirements, and puts forward a hypothesis. The second chapter presents the research methodology, identifies the participants of the empirical research, data collection sources, data collection methods, methods of ensuring the reliability of qualitative research data. In the third chapter, the data obtained during the expert investigation is summarized and systematized, the hypothesis is confirmed or rejected, conclusions are drawn, the objective information system cyber security assessment model is created and refined based on a theoretical and empirical research, the directions for improvement of the information system cyber security assessment process are identified, proposals are presented for the objective information system cyber security evaluation.

Key words: Cybersecurity, Cybersecurity Assessment, Compliance, Information system, Information system security assessment

SANTRAUKA

Parnarauskienė A. (2023) X informacinės sistemos vertinimas kibernetinio saugumo aspektu (magistro baigiamasis darbas). Vilnius Mykolo Romerio universitetas

Informacinės sistemos kibernetinio saugumo vertinimo tema aktuali organizacijoms, kurios valdo ir (ar) tvarko informacines sistemas, visuomenei ir valstybėms, kurių nacionalinis saugumas kasmet vis labiau priklauso nuo įvairių išorinių ir vidinių grėsmių, kylančio pavojaus kritinei informacinei infrastruktūrai. Mokslininkai, nagrinėdami informacinių sistemų kibernetinio saugumo vertinimo aspektus tyrinėja skirtingus faktorius, turinčius įtakos informacinių sistemų kibernetiniam saugumui, ieško atsakymų dėl kokių priežasčių atsiranda neatitikties (formalios atitikties) apraiškos. Daugelis mokslininkų mano, kad tik sukūrus veiksmingą informacinės sistemos kibernetinio saugumo vertinimo modelį galima objektyviai atlikti informacinės sistemos kibernetinio saugumo vertinimą. Todėl buvo iškelta pagrindinė tyrimo problema – kaip, taikant šiuolaikines mokslines strategijas, gerosios praktikos metodus, objektyviai atlikti informacinės sistemos kibernetinio saugumo vertinimą? Tyrimo objektas – informacinės sistemos kibernetinio saugumo vertinimo procesas. Tyrimo tikslas – sukurti objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelį, pateikti siūlymus objektyviam informacinių sistemų kibernetinio saugumo vertinimui atlikti. Tyrimo uždaviniai: išanalizavus mokslinę literatūrą, teorines strategijas, tarptautinę gerąją praktiką, teisės aktuose nustatytus reikalavimus, nustatyti informacinės sistemos kibernetinio saugumo vertinimo proceso imtį, sukurti objektyvaus informacinės sistemos kibernetinio saugumo vertinimo modelį, empiriškai jį patikrinti, įvertinti modelio taikymo praktikoje galimybes ir pateikti siūlymus objektyviam (ne formaliam) informacinės sistemos kibernetinio saugumo vertinimui atlikti. Tyrimo metodika: sisteminė mokslinės literatūros, mokslinių tyrimų, gerosios praktikos metodų, Europos ir Lietuvos teisės aktų, kitų dokumentų analizė, atvejo analizė, kokybinio tyrimo (ekspertinės apklausos) turinio analizė ir gautų duomenų sisteminė turinio analizė.

Empirinio tyrimo metu buvo iškelta pagrindinė hipotezė: gerosios praktikos metodai turi teigiamą įtaką informacinės sistemos kibernetiniam saugumui ir visos organizacijos kibernetiniam saugumui. Atlikus kokybinį tyrimą buvo patvirtinta ši hipotezė – visi ekspertai (informacinių sistemų valdytojų, tvarkytojų, kompetentingos institucijos (NKSC) atstovai patvirtino, kad gerosios praktikos metodų taikymas praktikoje didina organizacijos kibernetinį saugumą, brandą. Tyrimo metu buvo nustatyti pagrindiniai objektyvaus informacinės sistemos kibernetinio saugumo vertinimo elementai, neatitikties kibernetinio saugumo reikalavimams atsiradimo priežastys, identifikuotos informacinių sistemų kibernetinio saugumo vertinimo proceso tobulinimo kryptys.

Magistro baigiamojo darbo pabaigoje pateikiamos išvados ir siūlymai dėl objektyvaus informacinės sistemos kibernetinio saugumo vertinimo atlikimo ir proceso tobulinimo krypčių.

SUMMARY

Parnarauskienė A. (2023) Assessment of X Information System at Cyber Security Aspects (master thesis). Vilnius: Mykolas Romeris University

The topic of information systems cyber security assessment is relevant for organizations that own and/or manage information systems, for society and states whose national security every year increasingly depends on various external and internal threats that pose a threat to critical information infrastructure. Researchers, examining the aspects of the information systems cyber security assessment, study different factors that influence the cyber security of information systems, look for answers to the reasons for non-compliance (formal compliance) appearances. Many researchers believe that only if an effective information system cyber security assessment model is created, it is possible to objectively conduct an information system cyber security assessment. Therefore, the main research problem was raised - how to objectively perform an information system cyber security assessment using modern scientific strategies and best practice methods? The object of the study is the process of evaluating the cyber security of the information system. The purpose of the research is to create a model of objective information systems cyber security assessment, to provide proposals for objective information systems cyber security assessment. Research tasks: after analysing the scientific literature, theoretical strategies, international good practice, the requirements established in the theses, determine the sample of the information system cyber security assessment process, create an objective information system cyber security assessment model, empirically verify it, evaluate the possibilities of applying the model in practice and make proposals for an objective (non-formal) information system cyber security assessment. Research methodology: systematic analysis of scientific literature, scientific research, best practice methods, European and Lithuanian legal acts, other documents, case analysis, content analysis of qualitative research (expert survey) and systematic content analysis of the obtained data.

During the empirical study, the main hypothesis was put forward: good practice methods have a positive influence on the cyber security of the information system and the cyber security of the entire organization. After conducting a qualitative study, the following hypothesis was confirmed – all experts (representatives of owners and managers of information systems, representatives of the competent authority (NCSC) confirmed that the application of good practice methods in practice increases the organization's cyber security. Reasons for the emergence of non-compliance cyber security requirements, identified directions for improving the cyber security assessment process of information systems.

At the end of the master's thesis, conclusions and suggestions are presented regarding the performance of an objective (non-formal) information system cyber security assessment.

PRIEDAI

1 PRIEDAS

Informacinės sistemos vertinimo kibernetinio saugumo aspektu modelio empirinio tyrimo klausimynas ekspertams (I).

Gerbiamas eksperte, dėkoju Jums, kad sutikote dalyvauti mano atliekamame moksliniame tyrime, kuris organizuojamas rengiant magistro darbą tema „Informacinės sistemos vertinimas kibernetinio saugumo aspektu“. Empirinio tyrimo metu surinkta informacija, neatskleidžiant respondentų tapatybės, bus apibendrinta ir paskelbta rengiamame magistro darbe.

Empirinis tyrimas yra suskirstytas į 2 logines dalis:

- Pirmoji dalis (1 – 3 klausimai) remiasi atlikta moksline literatūros analize. Jums bus pateikti klausimai apie informacinių sistemų kibernetinio saugumo vertinimo procesą ir jo įgyvendinimo problematiką.
- Antroji dalis (4 – 8 klausimai) remiasi empirinio tyrimo gautais rezultatais.

Tyrimo tikslas – sužinoti ekspertų nuomonę apie informacinių sistemų kibernetinio saugumo vertinimą, proceso apimtį, vertinimo proceso problematiką.

Atsižvelgiant į tyrimo metu gautus respondentų rezultatus siekiama sukurti informacinės sistemos kibernetinio saugumo vertinimo modelį, kuris leistų organizacijai objektyviai įvertinti informacinės sistemos kibernetinį saugumą, objektyviai atlikti informacinės sistemos atitikties kibernetinio saugumo reikalavimams vertinimus.

Dėkoju už Jūsų skirtą laiką
Alina Parnarauskiene

PIRMOJI DALIS. Informacinės sistemos kibernetinio saugumo vertinimo proceso, kaip reiškinio, teorinis pagrindimas ir problematika.

1. Klausimas. *Jūsų nuomone, kokią reikšmę informacinės sistemos kibernetiniam saugumui turi:*

1.1. techninių priemonių (pvz. techninės ir programinės įrangos inventorizavimo, leistinos įrangos kontrolės, kenksmingo kodo aptikimo, įvykių auditavimo ir kt.) diegimas ir naudojimas;
1.2. organizacinių priemonių (pvz. techninės ir programinės įrangos valdymo, ryšių ir tinklų valdymo, incidentų valdymo, veiklos tęstinumo, personalo saugumo valdymo (mokymų) ir pan. procedūrų) nustatymas ir taikymas;
1.3. fizinės aplinkos saugumui skirtų priemonių diegimas ir naudojimas;
1.4. saugos nuostatų ir (ar) kitų saugos politiką įgyvendinančių dokumentų kokybė, jų aktualumas ir atitiktis teisės aktuose nustatytiems reikalavimams;
1.5. technologinio pažeidžiamumo testavimų (*penetration testing*) atlikimas;
1.6. darbuotojų ir fizinės aplinkos atsparumo kibernetinėms grėsmėms testavimų atlikimas (pvz. socialinės inžinerijos metodu);
1.7. rizikų vertinimas.

2. Klausimas. *Kaip manote, ar gerosios praktikos standartų (pvz. ISO/IEC 27001, NIST Cyber security framework, CIS Controls) metodų taikymas organizacijos veikloje gali turėti įtakos informacinės sistemos kibernetiniam saugumui?*

3. Klausimas. *Kaip manote, dėl kokių priežasčių daugelis organizacijų turi formaliai apsibrėžę informacinių sistemų saugos dokumentus, periodiškai neatlieka informacinių sistemų (informacinių technologijų) atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimų?*

ANTROJI DALIS. Informacinės sistemos kibernetinio saugumo vertinimo proceso imties nustatymas ir informacinių sistemų (informacinių technologijų) atitikties kibernetinio saugumo reikalavimams vertinimas.

4. Klausimas. *Kokias žemiau išvardintas veiklas atliekate vertindami informacinių sistemų kibernetinį saugumą, informacinių technologijų atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams?*

4.1. įdiegtų techninių priemonių vertinimą;
4.2. nustatytų organizacinių priemonių vertinimą;
4.3. fizinės aplinkos saugumo vertinimą;
4.4. saugos nuostatų ir kitų saugos politiką įgyvendinančių dokumentų aktualumo ir atitikties teisės aktuose nustatytiems reikalavimams vertinimą;
4.5. technologinio pažeidžiamumo testavimų (*penetration testing*) vertinimą;
4.6. darbuotojų ir fizinės aplinkos atsparumo kibernetinėms grėsmėms testavimų (pvz. soc. inžinerijos metodu) vertinimą;
4.7. rizikų vertinimą.
4.8. kitas veiklas *(nurodykite kokias)*.

5. Klausimas. *Jūsų nuomone, kokias veiklas reikėtų atlikti, kokias priemones reikėtų taikyti siekiant organizacijai objektyviai įvertinti, ar yra įgyvendinami informacinės sistemos saugos dokumentuose nustatyti organizaciniai ir techniniai kibernetinio saugumo reikalavimai?*

6. Klausimas. *Kokius metodus ir (ar) priemones taikote atlikdami:*

6.1. informacinių sistemų kibernetinio saugumo vertinimus, informacinių technologijų atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimus?
6.2. rizikų vertinimus?

7. Klausimas. *Kokių informacinių sistemų kibernetinio saugumo vertinimo priemonių ar rekomendacijų pasigendate Lietuvos nacionaliniuose teisės aktuose?*

8. Klausimas. *Jūsų nuomone, kokios Nacionalinio kibernetinio saugumo centro teikiamos paslaugos organizacinių ir techninių kibernetinio saugumo reikalavimų stebėsenos ir vertinimo srityje galėtų būti tobulintinos ir kaip?*

8.1. informacinių sistemų saugos dokumentų projektų derinimo procesas;
8.2. informacinių sistemų techniniai kibernetinio saugumo būklės patikrinimai (*penetration testing*);
8.3. organizacinių ir techninių kibernetinio saugumo reikalavimų stebėsena.

2 PRIEDAS

Informacinės sistemos vertinimo kibernetinio saugumo aspektu modelio empirinio tyrimo klausimynas ekspertams (II).

Gerbiamas eksperte, dėkoju Jums, kad sutikote dalyvauti mano atliekamame moksliniame tyrime, kuris organizuojamas rengiant magistro darbą tema ,,Informacinės sistemos vertinimas kibernetinio saugumo aspektu“. Empirinio tyrimo metu surinkta informacija, neatskleidžiant respondentų tapatybės, bus apibendrinta ir paskelbta rengiamame magistro darbe.

Empirinis tyrimas yra suskirstytas į 2 logines dalis:

- Pirmoji dalis (1 – 3 klausimai) remiasi atlikta moksline literatūros analize. Jums bus pateikti klausimai apie informacinių sistemų kibernetinio saugumo vertinimo procesą ir jo įgyvendinimo problematiką.
- Antroji dalis (4 – 8 klausimai) remiasi empirinių tyrimų gautais rezultatais.

Tyrimo tikslas – sužinoti ekspertų nuomonę apie informacinių sistemų kibernetinio saugumo vertinimą, proceso apimtį, ir proceso įgyvendinimo problematiką.

Atsižvelgiant į tyrimo metu gautus respondentų rezultatus siekiama sukurti informacinės sistemos kibernetinio saugumo vertinimo modelį, kuris leistų organizacijai objektyviai įvertinti informacinės sistemos kibernetinį saugumą, objektyviai atlikti informacinės sistemos atitikties kibernetinio saugumo reikalavimams vertinimus.

Dėkoju už Jūsų skirtą laiką
Alina Parnarauskiene

PIRMOJI DALIS. Informacinės sistemos kibernetinio saugumo vertinimo proceso, kaip reiškinio, teorinis pagrindimas ir problematika.

1. Klausimas. *Jūsų nuomone, kokią reikšmę informacinės sistemos kibernetiniam saugumui turi:*

1.1. techninių priemonių (pvz. techninės ir programinės įrangos inventorizavimo, leistinos įrangos kontrolės, kenksmingo kodo aptikimo, įvykių auditavimo ir kt.) diegimas ir naudojimas.
1.2. organizacinių priemonių (pvz. techninės ir programinės įrangos valdymo, ryšių ir tinklų saugumo valdymo, incidentų valdymo, veiklos tęstinumo, personalo saugumo valdymo ir pan. procedūrų) nustatymas ir taikymas.
1.3. fizinės aplinkos saugumui skirtų priemonių diegimas ir naudojimas.
1.4. saugos nuostatų ir (ar) kitų saugos politiką įgyvendinančių dokumentų kokybė, jų aktualumas ir atitiktis teisės aktuose nustatytiems reikalavimams;
1.5. technologinio pažeidžiamumo testavimų (*penetration testing*) atlikimas;
1.6. darbuotojų ir fizinės aplinkos atsparumo kibernetinėms grėsmėms testavimų atlikimas (pvz. socialinės inžinerijos metodu).
1.7. rizikos vertinimas.

2. Klausimas. *Kaip manote, ar gerosios praktikos standartų (pvz. ISO/IEC 27001, NIST Cyber security framework, CIS Controls) metodų taikymas organizacijos veikloje gali turėti įtakos informacinės sistemos kibernetiniam saugumui?*

3. **Klausimas.** *Kaip manote, dėl kokių priežasčių daugelis organizacijų turi formaliai apsibrėžę informacinių sistemų saugos dokumentus, periodiškai neatlieka informacinių sistemų (informacinių technologijų) atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimų?*

ANTROJI DALIS. Informacinės sistemos kibernetinio saugumo vertinimo proceso imties nustatymas ir informacinių sistemų (informacinių technologijų) atitikties kibernetinio saugumo reikalavimams vertinimas.

4. Klausimas. *Jūsų nuomone, kokias žemiau išvardintas veiklas reikėtų atlikti vertinant informacinės sistemos kibernetinį saugumą, informacinių technologijų atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams?*

4.1. įdiegtų techninių priemonių vertinimą.
4.2. nustatytų organizacinių priemonių vertinimą.
4.3. fizinės aplinkos saugumo vertinimą.
4.4. saugos nuostatų ir kitų saugos politiką įgyvendinančių dokumentų aktualumo ir atitikties teisės aktuose nustatytiems reikalavimams vertinimą;
4.5. technologinio pažeidžiamumo testavimų (*penetration testing*) vertinimą;
4.6. darbuotojų ir fizinės aplinkos atsparumo kibernetinėms grėsmėms testavimų (pvz. soc. inžinerijos metodu) vertinimą.
4.7. rizikų vertinimą.
4.8. kitas veiklas *(nurodykite kokias).*

5. Klausimas. *Jūsų nuomone, kokias veiklas reikėtų atlikti, kokias priemones reikėtų taikyti siekiant organizacijai objektyviai įvertinti, ar yra įgyvendinami informacinės sistemos saugos dokumentuose nustatyti organizaciniai ir techniniai kibernetinio saugumo reikalavimai?*

6. Klausimas. *Kokius metodus ir (ar) priemones siūlytumėte taikyti siekiant objektyviai atlikti:*

6.1. informacinių sistemų kibernetinio saugumo vertinimus, informacinių technologijų atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimus?
6.2. rizikų vertinimus?

7. Klausimas. *Kokių informacinių sistemų kibernetinio saugumo vertinimo priemonių ar rekomendacijų pasigendate Lietuvos nacionaliniuose teisės aktuose?*

8. Klausimas. *Jūsų nuomone kokios Nacionalinio kibernetinio saugumo centro teikiamos paslaugos organizacinių ir techninių kibernetinio saugumo reikalavimų stebėsenos ir vertinimo srityje galėtų būti tobulintinos ir kaip?*

8.1. informacinių sistemų saugos dokumentų projektų derinimo procesas;
8.2. informacinių sistemų techniniai kibernetinio saugumo būklės patikrinimai (*penetration testing*);
8.3. organizacinių ir techninių kibernetinio saugumo reikalavimų stebėsena.

3 PRIEDAS

8 lentelė Privalomų informacinių sistemų kibernetinio saugumo elementų, informacijos saugumo valdymo elementų, organizacinių ir techninių priemonių kategorijų bei kibernetinei gynybai skirtų saugumo kontrolės priemonių palyginimas

Nr.	Lietuvos nacionalinėje teisėje nustatyti minimalūs RIS kibernetinio saugumo valdymo elementai	Minimalūs privalomi kibernetinio saugumo elementai pagal TIS 2 direktyvos 21 straipsnio 2 dalį	ISVS privalomi minimalūs informacijos saugumo valdymo elementai	Organizacinių ir techninių priemonių kategorijos pagal NIST CSF	SANS CSC V.8* kibernetinei gynybai skirtos saugumo kontrolės priemonės
1	2	3	4	5	6
1.	Rizikų valdymas	Rizikos analizė ir informacinių sistemų saugumo politika	Informacijos saugumo politika (A.5)	Verslo aplinka (ID.BE) Rizikos valdymo strategija (ID.RM) Rizikos vertinimas (ID.RA)	07_Tęstinis pažeidžiamumų vertinimas ir taisymas
2.	Elektroninės informacijos ir duomenų saugumo valdymas	Incidentų valdymas	Informacijos saugumo incidentų valdymas (A.16)	Anomalijos ir įvykiai (DE.AE) Reagavimo planavimas (RS.RP) Komunikacija (RS.CO) Analizė (RS.AN) Pasekmių švelninimas (RS.MI)	17_Reagavimas į incidentus ir jų valdymas
3.	Veiklos atkūrimo valdymas	Veiklos tęstinumas ir krizių valdymas	Veiklos tęstinumo valdymo informacijos saugumo aspektai (A.17)	Veiklos atstatymo planas (RC.RP), Pasekmių švelninimas (RC.IM), Komunikacija (RC.CO)	11_Duomenų atkūrimo pajėgumai
4.	Paslaugų teikėjų valdymas	Tiekimo grandinės saugumas (tiekėjų valdymas)	Santykiai su tiekėjais (A.15)	Tiekimo grandinės (Tiekėjų) rizikos valdymas (ID.SC)	15_Tiekėjų valdymas
5.	Paslaugų valdymas	Įsigijimo, plėtojimo ir priežiūros saugumas, pažeidžiamumų valdymas ir atskleidimas	Sistemų įsigijimas, kūrimas ir priežiūra (A.14)	Priežiūra (PR.MA), Aptikimo procesai (DE.DP)	08_Audito įrašų stebėjimas, analizė ir saugojimas, 12_Tinklo infrastruktūros valdymas
6.	Elektroninės informacijos ir duomenų valdymas (saugos dokumentų kokybės vertinimas)	Politika ir procedūros, skirtos kibernetinio saugumo rizikos valdymo priemonių veiksmingumui įvertinti	Atitiktis (A.18)	Informacijos apsaugos procesai ir procedūros (PR.IP), Tobulinimas (RS.IM)	03_Duomenų apsauga,

Šaltinis: parengta šio darbo autorės

8 lentelės tęsinys kitame lape

8 lentelės tęsinys

7.	Teisinių ir organizacinių priemonių valdymas	Kibernetinės higienos praktika ir kibernetinio saugumo mokymai,	Informacijos saugumo organizavimas (A.6) Darbo saugumas (A.12)	Valdymas (ID.GV), Saugumo nuolatinė stebėsena (DE.CM)	04_Saugios konfigūracijos programinei ir techninei įrangai numatymas 05_Paskyrų stebėjimas ir kontrolė
8.	Techninės ir programinės įrangos valdymas	Turto valdymas	Turto valdymas (A.8),	Turto valdymas (ID.AM)	01_Leistinų ir pašalinių įrenginių inventorizavimas, 02_Leidžiamos ir draudžiamos programinės įrangos inventorizavimas,
9.	Ryšių ir tinklų saugumo valdymas	Kriptografijos ir šifravimo naudojimas, Kelių veiksnių tapatumo nustatymo sprendimų, saugių balso, vaizdo ir teksto ryšių bei saugių avarinių ryšių sistemų subjekto viduje naudojimas, Kriptografijos ir šifravimo naudojimo politiką ir procedūros	Ryšių saugumas (A.13) Kriptografija (A.10)	Apsaugos technologijos (PR.PT) Duomenų saugumas (PR.DS)	09_Elektroninio pašto ir naršyklės apsauga, 13_Tinklo stebėsena, 18_Įsibrovimų testavimas
10.	Personalo valdymas	Žmogiškųjų išteklių saugumas,	Žmogiškųjų išteklių saugumas (A.7)	Sąmoningumas ir mokymai (PR.AT)	14_Saugumo srities gebėjimų vertinimas ir mokymas
11.	Aplinkos saugumo valdymas	Prieigos kontrolės politika	Prieigos valdymas (A.9) Fizinis ir aplinkos saugumas (A.11)	Tapatybės valdymas ir prieigos kontrolė (PR.AC)	06_Prieigos valdymas 10_Apsauga nuo kenksmingo kodo, 16_Taikomųjų programų saugumas

* nuoroda į CSC Controls V.8 versijos priemonių aprašymą, Prieiga per internetą: https://www.cisecurity.org/controls/cis-controls-list (tikrinta 2023-02-28)

3. PRIEDAS

9 lentelė Informacija apie Registrų ir valstybės informacinių sistemų registre registruotus objektus, jų valdytojus

2023 ataskaita

Valdymo sritis	Viso	Duomenų valdymo įgaliotinis		Nuostatai	Duomenų saugos nuostatai		Specifikacija		Priėmimo aktas		Sąveika	
		Nurodytas	Nenurodytas	Yra	Yra	Nėra	Yra	Nėra	Yra	Nėra	Nurodyta	Nenurodyta
Aplinkos ministerija												
Valstybės informacinės sistemos	25	22	3	25	23	2	19	6	17	8	19	6
Įsteigti iki 2023 m.	25	22	3	25	23	2	19	6	17	8	19	6
Registrai	9	8	1	9	9	0	9	0	9	0	9	0
Įsteigti iki 2023 m.	9	8	1	9	9	0	9	0	9	0	9	0
Ekonomikos ir inovacijų ministerija												
Valstybės informacinės sistemos	13	11	2	13	12	1	13	0	11	2	13	0
Įsteigti iki 2023 m.	13	11	2	13	12	1	13	0	11	2	13	0
Registrai	2	2	0	2	2	0	1	1	2	0	1	1
Įsteigti iki 2023 m.	2	2	0	2	2	0	1	1	2	0	1	1
Energetikos ministerija												
Valstybės informacinės sistemos	2	2	0	2	2	0	2	0	2	0	2	0
Įsteigti iki 2023 m.	2	2	0	2	2	0	2	0	2	0	2	0
Finansų ministerija												
Valstybės informacinės sistemos	28	27	1	28	27	1	25	3	24	4	25	3
Įsteigti iki 2023 m.	28	27	1	28	27	1	25	3	24	4	25	3
Registrai	5	5	0	5	5	0	5	0	4	1	5	0
Įsteigti iki 2023 m.	5	5	0	5	5	0	5	0	4	1	5	0
Kita												
Valstybės informacinės sistemos	10	9	1	10	10	0	6	4	5	5	6	4
Įsteigti iki 2023 m.	10	9	1	10	10	0	6	4	5	5	6	4
Registrai	1	0	1	1	1	0	0	1	1	0	0	1
Įsteigti iki 2023 m.	1	0	1	1	1	0	0	1	1	0	0	1
Krašto apsaugos ministerija												
Valstybės informacinės sistemos	1	1	0	1	1	0	1	0	1	0	1	0
Registrai	3	2	1	3	3	0	2	1	2	1	2	1
Įsteigti iki 2023 m.	3	2	1	3	3	0	2	1	2	1	2	1

1 / 3

Šaltinis: parengta šio darbo autorės pagal informaciją pateiktą Registrų ir valstybės informacinių sistemų registre, prieiga per internetą: https://registrai.lt/ataskaita/ , tikrinta 2023-02-20

9 lentelės tęsinys kitame lape

9 lentelės tęsinys

Kultūros ministerija												
Valstybės informacinės sistemos	14	13	1	14	14	0	11	3	10	4	11	3
Įsteigti iki 2023 m.	14	13	1	14	14	0	11	3	10	4	11	3
Registrai	2	1	1	2	1	1	2	0	2	0	2	0
Įsteigti iki 2023 m.	2	1	1	2	1	1	2	0	2	0	2	0
Lietuvos Respublikos Seimas												
Valstybės informacinės sistemos	10	8	2	10	9	1	8	2	6	4	8	2
Įsteigti iki 2023 m.	10	8	2	10	9	1	8	2	6	4	8	2
Registrai	1	1	0	1	1	0	1	0	1	0	1	0
Įsteigti iki 2023 m.	1	1	0	1	1	0	1	0	1	0	1	0
Lietuvos Respublikos Vyriausybė												
Valstybės informacinės sistemos	2	2	0	2	2	0	1	1	2	0	1	1
Įsteigti iki 2023 m.	2	2	0	2	2	0	1	1	2	0	1	1
Registrai	1	1	0	1	1	0	1	0	1	0	1	0
Įsteigti iki 2023 m.	1	1	0	1	1	0	1	0	1	0	1	0
Socialinės apsaugos ir darbo ministerija												
Valstybės informacinės sistemos	12	12	0	12	12	0	11	1	11	1	11	1
Įsteigti iki 2023 m.	12	12	0	12	12	0	11	1	11	1	11	1
Registrai	3	3	0	3	3	0	3	0	3	0	3	0
Įsteigti iki 2023 m.	3	3	0	3	3	0	3	0	3	0	3	0
Susisiekimo ministerija												
Valstybės informacinės sistemos	20	19	1	20	19	1	18	2	16	4	18	2
Įsteigti iki 2023 m.	20	19	1	20	19	1	18	2	16	4	18	2
Registrai	7	7	0	7	7	0	7	0	5	2	7	0
Įsteigti iki 2023 m.	7	7	0	7	7	0	7	0	5	2	7	0
Sveikatos apsaugos ministerija												
Valstybės informacinės sistemos	72	66	6	72	71	1	53	19	49	23	53	19
Įsteigti iki 2023 m.	72	66	6	72	71	1	53	19	49	23	53	19
Registrai	9	9	0	9	9	0	9	0	9	0	9	0
Įsteigti iki 2023 m.	9	9	0	9	9	0	9	0	9	0	9	0
Švietimo, mokslo ir sporto ministerija												

9 lentelės tęsinys kitame lape

9 lentelės tęsinys

Valstybės informacinės sistemos	25	23	2	25	23	2	20	5	16	9	20	5
Įsteigti iki 2023 m.	25	23	2	25	23	2	20	5	16	9	20	5
Registrai	10	10	0	10	10	0	9	1	9	1	9	1
Įsteigti iki 2023 m.	10	10	0	10	10	0	9	1	9	1	9	1
Teisingumo ministerija												
Valstybės informacinės sistemos	14	13	1	14	14	0	10	4	10	4	10	4
Įsteigti iki 2023 m.	14	13	1	14	14	0	10	4	10	4	10	4
Registrai	13	13	0	13	13	0	13	0	13	0	13	0
Įsteigti iki 2023 m.	13	13	0	13	13	0	13	0	13	0	13	0
Užsienio reikalų ministerija												
Valstybės informacinės sistemos	4	4	0	4	4	0	2	2	1	3	2	2
Įsteigti iki 2023 m.	4	4	0	4	4	0	2	2	1	3	2	2
Vidaus reikalų ministerija												
Valstybės informacinės sistemos	28	24	4	28	25	3	18	10	16	12	18	10
Įsteigti iki 2023 m.	28	24	4	28	25	3	18	10	16	12	18	10
Registrai	19	18	1	19	19	0	15	4	15	4	15	4
Įsteigti iki 2023 m.	19	18	1	19	19	0	15	4	15	4	15	4
Žemės ūkio ministerija												
Valstybės informacinės sistemos	18	15	3	18	16	2	15	3	13	5	15	3
Įsteigti iki 2023 m.	18	15	3	18	16	2	15	3	13	5	15	3
Registrai	9	8	1	9	8	1	9	0	9	0	9	0
Įsteigti iki 2023 m.	9	8	1	9	8	1	9	0	9	0	9	0