VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS

Magistro baigiamasis darbas

Kibernetinio saugumo proceso gebėjimo vertinimo modelio kūrimas ir validavimas

Creation and Validation of Cyber Security Process Capability Assessment Model

Tomas Martinkėnas

VILNIUS 2018

MATEMATIKOS IR INFORMATIKOS FAKULTETAS

INFORMATIKOS KATEDRA

Darbo vadovas Docentas dr. Antanas Mitašiūnas_____

Darbo recenzentas Linas Litvinas_____

Darbas apgintas _____

Darbas įvertintas _____

Registravimo NR. _____

Įrašoma atidavimo į katedrą data_____

Kibernetinio saugumo proceso gebėjimo vertinimo modelio kūrimas ir validavimas

Santrauka

Universalaus kibernetinio saugumo proceso gebėjimo vertinimo modelio nėra. Šiame darbe ISO/IEC 33071 standartas yra praplečiamas kibernetinio saugumo inžineriniais procesais taip sukuriant universalų kibernetinio saugumo proceso gebėjimo vertinimo modelį. Jo inžinerinių procesų kategorija padalinta į penkias dalis pagrįstas geriausiomis praktikomis ir standartais inkorporuojant rizikų valdymą. Šios dalys yra: identifikavimas, apsauga, aptikimas, reagavimas, atsistatymas. Kiekviena iš dalių sudaryta kruopščiai atrenkant ir sudarant atitinkamus kibernetinio saugumo procesus. Pasitelkiant ISO/IEC 33020 standartą sudarytas kibernetinio saugumo proceso gebėjimo vertinimo modelis yra panaudotas vertinti realios organizacijos veiklą taip pagrindžiant modelio adekvatumą. Sukurtas modelis darbe pavadintas CyberSPICE.

Raktiniai žodžiai: kibernetinis saugumas, procesas, proceso modelis, gebėjimo vertinimo modelis

Creation and Validation of Cyber Security Process Capability Assessment Model

Abstract

In the thesis cybersecurity engineering processes expand ISO/IEC 33071 creating a model for assessing cyber security process capability as thus fulfilling originated deficiency. Its engineering process divides into five parts based on cyber security best practices and standards incorporating risk based approach. These parts are as following, identification, protection, detection, response and recovery. Each part consists of carefully selected and treated cybersecurity activities or processes. Justifying the adequacy of the model itself, Cybersecurity Process Capability Assessment Model by means of ISO/IEC 33020 is used to evaluate the activities of real organization. A name of CyberSPICE is given to a new model.

Key words: cyber security, process, process model, capability assessment model.

Turinys

1. Įvadas

Nepaisant kylančių sunkumų ir brangstančių saugumo sprendimų, sudėtingėjančių technologijų apsaugoti informacijai ir turtui, organizacijos turi išlaikyti aukštą saugumo lygį, nes kibernetinės atakos kelia apčiuopiamą grėsmę reputacijai, finansams ar net žmonių gyvybėms. Per pastaruosius metus ne kartą kompanijos nukentėjo, kai milžiniškas kiekis klientų duomenų buvo nutekintas į viešą erdvę, verslo paslaptys ir intelektinė nuosavybė atskleista. Vis dažniau ir dažniau aptinkamas kenkėjiškas kodas sukurtas sugadinti pramonės industrijos kontrolės priemones. Kibernetinis karas tarp valstybių pasireiškia atvira forma.

Būtina apsiginti nuo atakų, siekiant išsaugoti turtą, tačiau saugumas savaime neatsiranda, reikia veiksnių, kurie jį įgalina, o išlaikyti aukštą saugumo lygį – dar sunkiau. Žmonės negali visiškai atsikratyti įgimto žmogiškojo faktoriaus ir yra pažeidžiami. Technologijos neišsprendžia šių problemų, o procesai dėl organizacijos poreikių dažniausiai yra orientuoti į greitį, o ne į saugumą. Organizacijos susiduria su problemomis ieškodamos talentingų darbuotojų. Sunku yra juos išlaikyti. Aplinka tampa vis labiau sudėtingesnė ir tarpusavyje susijusi, todėl pavienių sprendimų ar iniciatyvų nepakanka [29].

Iš kitos pusės, kibernetinių nusikaltėlių ir įsilaužėlių motyvacija yra didelė, jie yra „ginkluoti“ naujausiomis technologijomis, puikūs specialistai ir gerai finansuojami ne kaip pavieniai asmenys, o ištisos grupuotės. Skaičiuojama, jog pastangų įsilaužti, lyginant su pastangomis apsaugoti, reikia dešimt kartų mažiau. Nusikaltėlių nevaržo ilgi procesai, kurie dažni organizacijose, jų laikas nėra ribotas darbo valandomis, todėl besiginančioms organizacijoms tampa sunku spėti paskui su saugumo sprendimais ir to neužtenka – reikia būti žingsniu priekyje negailestingame kibernetiniame pasaulyje Dėl išvardintų priežasčių informacinių technologijų (IT) saugumo tema yra **aktuali** ir tampa kasdien vis aktualesnė.

Kibernetinio saugumo įgyvendinimas prasideda nuo vadovybės palaikymo [1]. Organizacijai kuriant strategiją būtina žinoti, koks saugumo lygis yra įgyvendinamas duotuoju laikotarpiu, kad galėtų užsibrėžti ir nuosekliai siekti aukštesnio. Tam reikalinga įsivertinti kibernetinio saugumo gebėjimą, t.y. reikia apibrėžti procesus, kaip veiksnius, kuriuos atlikus sukuriama tam tikra būsena. Kibernetinio saugumo proceso gebėjimo vertinimo modelis yra įrankis spręsti šį klausimą.

Universalaus kibernetinio saugumo proceso gebėjimo vertinimo modelio nėra. Egzistuoja keletas specifinių kibernetinio saugumo ar informacinio saugumo įgyvendinimo vertinimo modelių, tačiau visi jie daugiau ar mažiau orientuoti į tam tikrą sritį ar sektorių, iš kurio buvo gautas atitinkamas finansavimas [2][3].

Kibernetinio saugumo proceso gebėjimo vertinimo modelis teikia naudą organizacijoms. Jis leidžia įvertinti esamą padėtį, suprasti kaip kibernetinis saugumas padeda pasiekti organizacijos

strateginį tikslą, palengvina verslo pagrindu grįstas diskusijas su sprendimų priėmėjais. Modelį naudojant specialių veiksmų planavimui, siekiant pasiekti strateginį tikslą, galima prioretizuoti investicijas. Be viso to modelis geriausiai tinka pamatuoti, o taip pat palyginti organizaciją su kitais rinkos dalyviais [2]. Modelis taip pat veikia kaip katalizatorius – pasirinkus tam tikrą norimą pasiekti saugumo lygį ir jį pasitvirtinus, įpareigoja organizaciją tobulėti. Kartu modelis yra struktūrinis matas, leidžiantis organizacijai diskutuoti „bendra kalba“ apie uždavinius, tikslus, pasiekimus ir klaidas.

Šio darbo **tikslas** yra sukurti universalų modelį. Tai bus naujas kibernetinio saugumo proceso gebėjimo vertinimo modelis ir modelio adekvatumas bus pagrįstas darbe. Tikslui įgyvendinti yra iškeliami šie **uždaviniai**:

1. Išnagrinėti į procesus orientuotos veiklos procesų gebėjimo vertinimo ir gerinimo metodus.
2. Sukurti kibernetinio saugumo proceso gebėjimo vertinimo modelį.
3. Pagrįsti kibernetinio saugumo proceso gebėjimo vertinimo modelio adekvatumą.
4. Nustatyti organizacijos kibernetinio saugumo proceso esamą gebėjimo profilį.

Išnagrinėjus į procesus orientuotos veiklos procesų gebėjimo vertinimo ir gerinimo metodus, identifikavus ir sukūrus pagrindą būdingiems kibernetinio saugumo procesams, bus sudarytas kibernetinio saugumo proceso etaloninis modelis [4]. Atitinkamai bus sukurtas kibernetinio saugumo proceso gebėjimo vertinimo modelis ir pagrįstas jo adekvatumas remiantis organizacijos praktika. Universalaus kibernetinio saugumo gebėjimo brandos modelio nėra ir tai pagrindžia temos **naujumą**.

Darbo rezultate pagal kibernetinio saugumo proceso gebėjimo vertinimo modelį bus nustatytas pasirinktos organizacijos gebėjimo profilis. Proceso gebėjimo vertinimo modelis pasitarnaus sudaryti organizacijos tikslinį gebėjimo profilį. Šie žingsniai dar kartą leis patikrinti modelio validumą. Dalinai pagrįstas modelis turi užpildyti universalaus kibernetinio saugumo proceso gebėjimo vertinimo modelio spragą.

2. Literatūros apžvalga

Literatūros apžvalgoje aprašoma susijusi ir artima kibernetinio saugumo proceso modeliui mokslinė literatūra, kuri bus panaudota moksliniam tiriamajam darbui ir modelio sudarymui. Gilinantis į skirtingą medžiagą paaiškėjo, jog kibernetinio saugumo sąvoka nėra visuotinai vieningai suprantama. Teisiniuose aktuose sąvoka apibrėžiama vienaip, standartuose – kitaip, o visuomenėje – dar kitaip. Priešingai nei informacinio saugumo sąvoka, kuri yra senesnė ir nusistovėjusi standartų dokumentacijoje. To pasekoje nagrinėti kibernetinio saugumo sąvokai skirtas atskiras skyrius literatūros apžvalgos pradžioje. Apibrėžta sąvoka bus naudinga tikslinio modelio sudarymui.

2.1. Kibernetinio saugumo sąvoka

Kompiuterių tinklai apgaubė visą pasaulį. Technologija stipriai praplėtė galimybių ribas leidžiančias dirbti našiau, gyventi patogiau, ilsėtis įdomiau, spręsti problemas efektyviau. Kartu su informacinėmis technologijomis kompiuteriniai tinklai gyventojams, įmonėms, organizacijoms, galų gale valstybėms tampa veiksmingais ekonominės ir socialinės gerovės didinimo įrankiais.

Kompiuterinių tinklų galimybės auga ir toliau. Didėja jų reikšmė visose žmonių gyvenimo srityse. Kompiuterių tinklai yra atviri ir išnaudojami įvairiausiai naudą nešančiai veiklai. Kaip bebūtų, kompiuterių tinklais, tokia galinga jėga, naudojasi ir piktavaliai atlikti savo kenkėjiškus, pavojų keliančius darbus. Tokios blogos veiklos pavyzdys galėtų būti technologinių, ekonominių ar socialinių informacijos valdymo sistemų darbo trikdymas, neteisėtas informacijos, didžiausio šiuolaikinio pasaulio turto, grobimas ir nelegali sklaida.

Atakų metu, pavyzdžiui, siunčiamas didelis kiekis užklausų iš įvairių prie interneto prijungtų užgrobtų įrenginių, taip siekiant sutrikdyti kompiuterių tinkle veikiančias sistemas. Per trumpą laiką – vos trejus metus – toks atakos vektorius piktavalių buvo patobulintas iš esmės net kelis kartus. Iš pradžių atlikti galingą ataką naudoti kenkėjiškomis programomis užkrėsti ir pilnai valdomi kompiuteriai. Kad ataka būtų įvykdyta, vos išsivysčius ir patobulėjus „debesų“ technologijoms, įsilaužėliams pakakdavo gauti prieigą prie milžiniškus skaičiavimo resursus turinčių mašinų [6]. Paplitus interneto įrenginiams, paprasčiausi prietaisai, pradedant internetinėmis kameromis baigiant sudėtingomis išmanių namų valdymo sistemomis, turintys pažeidžiamumus pradėti naudoti masinėms atakoms įgyvendinti [7].

Tokių kibernetinių grėsmių šaltinis gali būti priešiškos valstybės, teroristinės organizacijos, organizuotos nusikalstamos grupuotės, pavieniai programuotojai, tiesiog vagys. Vadinamosios kibernetinės atakos tapo nauju, moderniu, dar daug kam nežinomu ir pilnai nesuprantamu

pavojingu ginklu, galinčiu paralyžiuoti ne tik atskirų įstaigų, gamybos, prekybos, transporto, ryšių, gydymo, elektros, vandens tiekimo įmonių, bet net ir valstybių veiklą [7].

Siekiant sumažinti ir valdyti riziką susijusią su kibernetinėmis grėsmėmis, organizacijos turi rūpintis saugumu. Saugumas susijęs su grėsmėmis internetinėje erdvėje literatūroje dažnai skirstomas į dvi sritis: informacinį saugumą ir kibernetinį saugumą. Iš pirmo žvilgsnio, skirtumas pasireiškia kylančių grėsmių ir rizikos valdymo atžvilgiu, tačiau suprasti teisingai reikia pasigilinti į abi sąvokas.

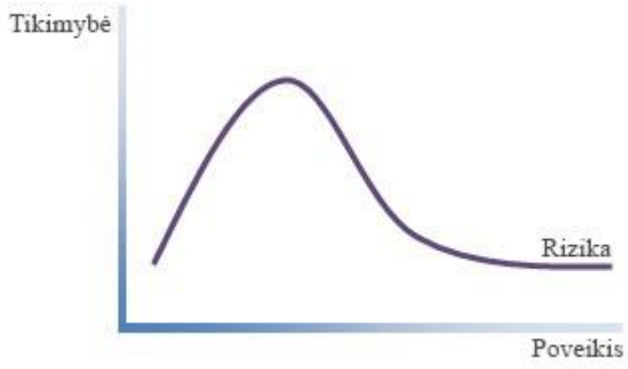
Kadangi informacinio saugumo terminas yra senas ir nusistovėjęs standartuose, galima pradėti nuo jo. Ši sritis apibrėžiama kaip informacijos ir infrastruktūros gerovės būsena, kurioje informacijos ir paslaugų vagystės, klastojimo, naikinimo tikimybė yra laikoma žemame arba toleruojamame lygyje. Šis apibrėžimas remiasi penkiais pagrindiniais elementais, kurie yra informacijos (1) konfidencialumas, (2) vientisumas, (3) pasiekiamumas, (4) autentiškumas ir (5) galimybės nepripažinti nebuvimas[1]. Tai yra praplėstas ir modernus klasikinio informacijos saugumo apibrėžimas, kuriame dėmesys kreipiamas tik į tris pagrindinius komponentus, t. y. duomenų konfidencialumą, vientisumą ir pasiekiamumą [8][20].

Informacinio saugumo terminas ir jo supratimas yra nusistovėjęs ir toks, ar kiek pakoreguotas, randamas mokslinėje literatūroje, geriausioje praktikoje, o tuo metu kibernetinio saugumo terminas – dar naujas ir keliantis daug diskusijų. Literatūros apžvalgoje kibernetinis saugumas bus nagrinėjamas keliais aspektais: iš rizikų perspektyvos ir taip pat vertinami įvairiuose teisės aktuose sukurti apibrėžimai.

Pradedant nuo rizikų perspektyvos, pirmiausia reikia apibrėžti terminą kibernetinė rizika. Kibernetinė rizika nėra viena specifinė rizika. Tai rizikų grupė, kuri išsiskiria sofistikuota technologija, sudėtingais atakos vektoriais, savo reikšme ir poveikiu. Ši rizikos grupė pasižymi ir dviem daugiausiai panašiais charakteristikos bruožais: (a) turi didelį potencialų poveikį ir (b) rizikos priskiriamos kibernetinėms kadaise buvo traktuojamos kaip neįtikėtinos [23].

Siekiant suprasti, reikėtų pradėti nuo tradicinės rizikos kreivės grafiško atvaizdavimo. 1 pav. yra paprastas grafikas vaizduojantis koreliaciją tarp rizikos atsitikimo tikimybės ir potencialaus poveikio. Grafiko kreive judant į dešinę, rizikos potencialus poveikis didėja. Kairėje rizikos grafiko pusėje pažymėta grupė rizikų, turinti labai aukštą poveikį ir labai žemą tikimybę įvykti. Taip jau yra, jog organizacijos dažniausiai yra suvaržytos savo resursų ir dėmesį bei pastangas kreipia į rizikų grupę, kuri pasižymi didele atsitikimo tikimybe ir potencialiai reikšmingu poveikiu.

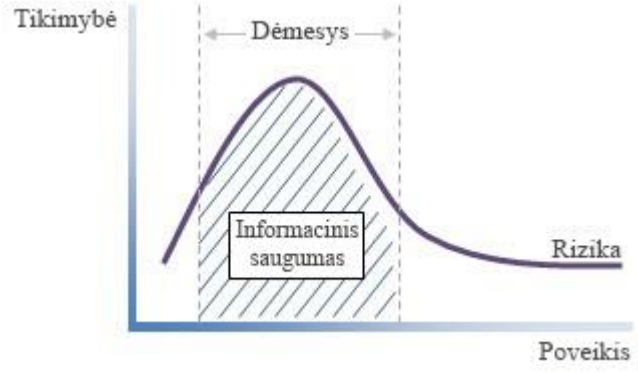
[1] Šių elementų detalūs paaiškinimai pridedami darbo priede Nr. 1.



1 pav. Priklausomybė tarp rizikos atsitikimo tikimybės ir potencialaus poveikio.

Toliau reikia apsibrėžti, kur organizacijos kreipia savo resursus ir pastangas rizikai suvaldyti (vaizduojama 2 pav.). Rizikos tolerancijos lygis priklauso nuo tokių faktorių kaip rizikos apetitas, kaštų efektyvumas, vadovybės požiūris, organizacinė kultūra, resursų pasiekiamumas ir santykinis grėsmių žemėlapis.

Kaip iliustruojama žemiau, pastangos skiriamos suvaldyti prioretizuotoms rizikoms yra dažniausiai priskiriamos informacinio saugumo sričiai. Tarp šių rizikų pagal informacinio saugumo apibrėžimą patenka tradicinės kenkėjiškos programos (virusai, sekimo programinė įranga, kenkėjiškos reklamos ir t.t.), standartinės duomenų vagystės atakos, paslaugų sutrukdymo atakos, įsilaužėlių veiksmai ir pan.

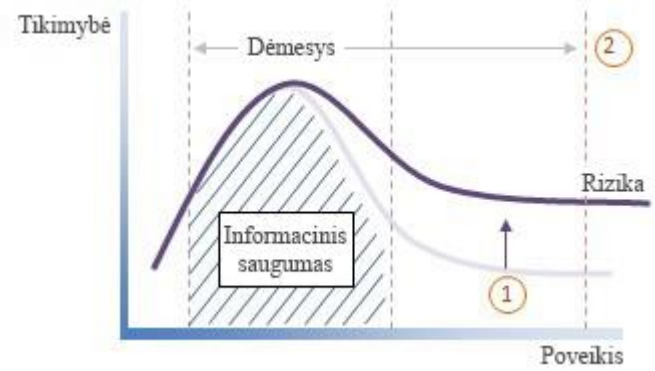


2 pav. Organizacijų nukreipti resursai suvaldyti rizikai.

Technologijoms tobulėjant ir kartu nykstant galimybių ribai daug kas pasikeitė. Grėsmių žemėlapis taip pakito, jog rizikos, kurios anksčiau buvo laikytos mažai tikėtinomis pradėjo reikštis dažniau ar net reguliariai. Padidėjusi tikimybė labai aukštą poveikį turinčių rizikų pavaizduota 3 pav. 1-u numeriu.

Tokį tendencijos pasikeitimą galima priskirti brandesniems atakos įrankiams ir metodams, padidėjusiam poveikiui, sustiprėjusiai įsilaužėlių motyvacijai ir tobulesniems atakų aptikimo įrenginiams, įgalinantiems didesnį skaidrumą. Galima teigti, jog toks pasikeitimas yra didėjančio sąmoningumo šioms sofistikuotoms rizikoms rezultatas.

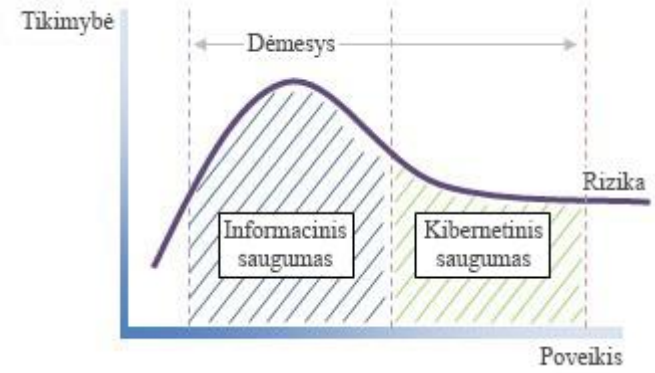
3 pav. 2-u numeriu yra pavaizduota tai, kaip pokyčiai grėsmių žemėlapyje verčia organizacijas plėsti prioretizuotų rizikų grupę tam, kad atsižvelgti į šias anksčiau praleistas rizikas [9].



3 pav. Padidėjusi labai aukštą poveikį turinčių rizikų tikimybė.

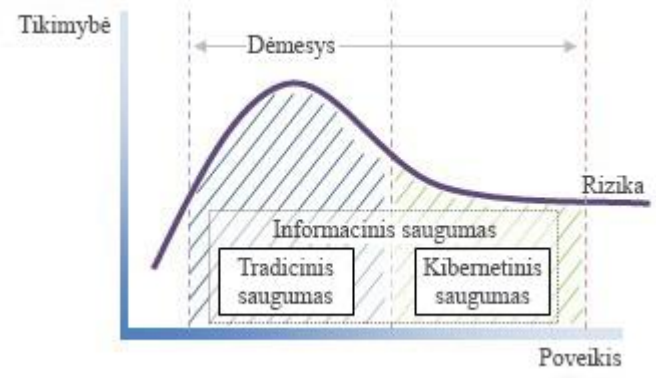
Ši nauja grupė rizikų turinčių labai didelį poveikį ir reikalaujančių organizacijos dėmesio yra dažnai apibūdinama kaip kibernetinė rizika. Kaip pavaizduota 4 pav., pastangos skirtos suvaldyti kibernetinę riziką yra žinomos kaip kibernetinis saugumas ar kibernetinė sauga.

Nagrinėjama grupė rizikų apibrėžiama įvairiais nekasdieniškais scenarijais: organizacijos specifika, specialiai sukurta kenkėjiška programine įranga, programinės ir fizinės įrangos manipuliacija, pavogtų kredencialų panaudojimu, šnipais ir informacijos tekintojais, pažeidžiamumo archajiškose sistemose išnaudojimu, trečių šalių tiekėjų atakomis ir t.t. Dar kitaip – tai sofistikuotos atkaklių piktavalių atakoms.



4 pav. Kibernetinis saugumas kaip pastangos suvaldyti kibernetinę riziką.

Žinant atskirus informacinio saugumo ir kibernetinio saugumo apibrėžimus būtų galima pagalvoti, jog tai yra dvi skirtingos disciplinos, tačiau taip remiantis ISACA metodologija nėra ir kibernetinis saugumas turi būti laikomas informacinio saugumo dalimi.



5 pav. Kibernetinis saugumas kaip dalis informacinio saugumo.

Pagal nagrinėtą medžiagą, galima teigti, jog kibernetinis saugumas yra suma pastangų adresuotų suvaldyti kibernetinę riziką, kurios didžioji dalis dar visai neseniai buvo laikoma kaip nereikalaujanti didelio dėmesio. Reikia turėti omenyje, jog toks rizikų pokytis atspindi šiuo metu pasirodančias tendencijas. Labai didelį poveikį turinčios rizikos taps vis dažniau ir dažniau įvykstančios, o tai savaime suprantama vers organizacijas dar labiau ginti savo turtą ir kurti kūrybingus sprendimus kaip tas rizikas suvaldyti. Tam kad suprasti kibernetinio saugumo reikšmę, pirmiausia reikia suprasti kibernetinę riziką [21].

Apibendrinant šią dalį galima suformuluoti kibernetinio saugumo sąvoką remiantis rizikomis – tai įvairiausių technologijų panaudojimas ir procesai, kurie leidžia apsaugoti tinklus, kompiuterius, programas ir duomenis nuo atakų, žalos ar neautorizuotų prieigų remiantis rizikos valdymo procesu [10]. Šį apibrėžimą galima palyginti su kitoje literatūroje ar teisės aktuose apibrėžta kibernetinio saugumo sąvoka.

Pagal D. Shoemakerį ir A. Conkliną, kibernetinis saugumas yra procesų visuma, kurie susiję su kylančių kibernetinių grėsmių identifikavimu bei sąnaudomis pagrįstu kontrpriemonių taikymu, kūrimu ir palaikymu [11].

Lietuvos kibernetinio saugumo įstatyme sąvoka apibrėžiama plačiau. Čia kibernetinis saugumas – tai visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti [12]. NIST standarte, kuris plačiau nagrinėjamas literatūros apžvalgoje ir moksliniame tyrime, kibernetinio saugumo sąvoka apibrėžta beveik identiškai [13]. Palyginimas iš įvairių aspektų apibendrinamas 1-oje lentelėje.

Informacinio saugumo profesionalai užsiima saugumo pagrindais, kurie apima strategijos, politikų, procedūrų kūrimą, rizikos valdymą, įsilaužimų stebėjimą, saugumo sąmoningumo kėlimą, tinklų segmentavimą.	Kibernetinio saugumo profesionalus galima suskirstyti į dvi grupes: 1. Incidentų valdymo sritis, kuriai reikalingos gilios techninės žinios.

	2. Kibernetinė sauga, kai duomenys ir tinklai saugomi nuo kompiuterinių virusų, dar nežinomų kibernetinių atakų ir pan.
Informacinis saugumas taikomas bet kokiai informacijai neatsižvelgiant į jos formą.	Kibernetinė sauga taikoma kibernetinei erdvėje.
Popierinė duomenų forma yra informacinio saugumo objektas.	Popierinė duomenų forma nėra kibernetinio saugumo duomenų objektas.
Informacinis saugumas duomenis saugo nuo bet kokio tipo pavojų ir grėsmių.	Kibernetinis saugumas duomenis saugo nuo grėsmių kylančių kibernetinėje erdvėje.
Informacinis saugumo disciplinoje stengiamasi apsaugoti nuo neautorizuotų prieigų, duomenų atskleidimo, netinkamo panaudojimo, modifikavimo, paslaugų trikdymo.	Kibernetinio saugumo disciplina naudojama apsisaugoti nuo kibernetinių nusikaltimų, sukčiavimų ir vagysčių.

1 lentelė. Informacinio ir kibernetinio saugumo palyginimas.

Apžvelgiant įvairius šaltinius ryškėja skirtumas tarp informacinio saugumo ir kibernetinio saugumo. Kibernetinis saugumas yra struktūra skirta apsaugoti viską, kas yra pažeidžiama internetinių įsilaužimų, atakų ar neautorizuotų prieigų, ir ši struktūra pagrinde susideda iš kompiuterių, tinklų , serverių ir programų. Ne taip kaip informacinis saugumas, kibernetinis saugumas yra orientuotas į būtent skaitmeninių formų apsaugą.

Prie šios terminologijos ir skirtumų grįžtama mokslinio darbo procesų modelių palyginimo dalyje, kur yra lyginami ir grupuojami skirtingi kibernetinio saugumo ir informacinio saugumo procesų modeliai.

2.2. Susijusių šaltinių apžvalga

Vienas iš pagrindinių naudotų duomenų rinkimo metodų yra antrinių duomenų rinkimas ir analizė. Naudoti įvairūs tyrimų šaltiniai ir duomenys, taip pat mokslo produkcija, kuri buvo publikuota įvairių tarptautinių organizacijų vienijančių informacinį ar kibernetinį saugumą, egzistuojantys kibernetinio saugumo proceso modeliai, vertinimo modeliai, taip pat struktūriniai dokumentai.

Kaip ir minėta įžangoje, egzistuojantys kibernetinio saugumo vertinimo modeliai ar jų atitikmenys yra labai specifiniai, pritaikyti konkrečiam sektoriui ar taikytini valstybės mastu. Literatūros apžvalgoje atrenkami tinkamiausi modeliai ir jų dalys tolimesniam moksliniam tyrimui ir išvestinio kibernetinio saugumo proceso modelio sudarymui.

2.2.1. Kibernetinio saugumo vertinimo ir susiję modeliai

Padidėjęs sąmoningumas apie grėsmių žemėlapio sudėtines dalis, kartu ir poreikis atitikti tam tikrus nustatytus valstybės, industrijos ar kt. standartus, sukūrė poreikį vertinti ir raportuoti apie pasiruošimą suvaldyti kibernetines grėsmes. Tai galima daryti pasinaudojant egzistuojančiais kibernetinio saugumo vertinimo modeliais.

Gebėjimo vertinimo modelių ištakos prasideda programinės įrangos kūrimo industrijoje, kur modeliai tarnavo kaip rekomenduojamų patobulinimų organizacijoms, norinčioms pakelti programinės įrangos kūrimo proceso brandą, rinkinys [2]. Įprastai, gebėjimo brandos modelis turi du komponentus: (a) matavimo ir objekto reikšmes, kurios nurodo nuoseklaus kūrimo būdą paremtą hierarchine progresija, ir (b) kriterijus (tokius kaip būsenos, procesai ar aplikacijos tikslai) skirtus pamatuoti objektų gebėjimą. Apjungti šie komponentai suteikia brandos lygių seką objekto klasėms. Kitaip, gebėjimo brandos modelis atstoja numatomą, pageidaujamą arba tipišką tų objektų pokyčio kelią nusakytą diskrečiais etapais [5]. Modeliai leidžia organizacijoms ištirti savo gebėjimą paeiliui įvairiose dimensijose ir parodyti hierarchinę progresiją, tokiu būdu kuriant kriterijus, kurie atstovautų apibrėžtus brandos lygius.

Pradedant nuo tokių ankstyvų modelių pavyzdžių kaip *Organization for Standardization's Systems Security Engineering Capability Maturity Model (SSE-CMM), Citigroup's Information Security Evaluation Model (CITI-ISEM)* ir *Computer Emergency Response Team / CSO Online at Carnegie Mellon University (CERT/CSO)* amžių sandūroje atsirado modernios iniciatyvos tokios kaip dabartinis *International Organization for Standardization (ISO/IEC)* standartas, *the National Institute of Standards and Technology (NIST) Cybersecurity framework, the U.S. Department of Energy's Cybersecurity Capability Maturity Model (C2M2),* ir galiausiai *the U.S. Department of Homeland Security's NICE-CMM* publikuotas 2014-ais metais [6][22].

Jungtinių Amerikos Valstijų Energetikos departamento sukurtas ES C2M2, kartu su išvestiniais gebėjimo brandos modeliais C2M2 ir ONG-C2M2, pateikia brandos modelį ir įsivertinimo įrankį nustatyti kibernetinio saugumo pasiruošimo lygį energetikos produkcijos sektoriuje ir skirstomuosiuose tinkluose. Kaip bebūtų, šis įrankis yra specifinis ir pritaikytas energetikos pramonei, kas varžo jo panaudojimą.

Jungtinių Amerikos Valstijų Saugumo departamentas kartu su Programinės įrangos inžinerijos institutu *Carnegie Mellon* sukūrė modelį sutrumpintu pavadinimu NICE-CMM, kuris koncentruojasi į darbo jėgos plėtrą, procesų brandą ir veiklos atsparumo praktikas tam, kad padėtų organizacijoms kelti kibernetinio saugumo lygį. Kaip bebūtų, jungtinis darinys nesiūlo specifinių kibernetinio saugumo praktikų. Papildomi struktūriniai dokumentai turi būti įtraukti ir naudojami siekiant vertinti veiklą pagal šį modelį, todėl modelis nebus naudojamas kibernetinio saugumo proceso etaloninio modelio sudarymui.

NIST savanoriškas kibernetinio saugumo struktūros modelis sukurtas valdyti kibernetinio saugumo riziką susideda iš standartų ir geriausių praktikų. Kaip teigia patys autoriai, šis kibernetinio saugumo struktūros modelis prioretizuotu, prisitaikančiu ir kainos atžvilgiu efektyviu būdu leidžia prisidėti prie apsaugos ir atsparumo kritinėje infrastruktūroje ir kituose ekonomikai bei nacionaliniam saugumui svarbiuose sektoriuose [14].

Išvardinti modeliai ar papildantys šaltiniai padeda organizacijoms įsivertinti pasiruošimą atremti kibernetines atakas, bet dažniausiai teikia tik aukšto lygio patarimus ir taikomus tik labai specifinėse pramonės srityse. Rinkoje nėra universalaus kibernetinio saugumo gebėjimo brandos vertinimo modelio. Svarbi ir lemianti to priežastis gali būti finansavimo trūkumas. Dėl to, universalus modelis įgyja svarbią reikšmę, kad organizacijos nesusijusios su aprašytais sektoriais galėtų adekvačiai ir tinkamai įsivertinusios gebėjimą pasiruošti atremti gresiančias kibernetines atakas. Kitas svarbus dalykas yra tas, jog aprašyti egzistuojantys vertinimo modeliai yra orientuoti į kibernetinio saugumo būseną, o ne procesą. Taip yra dėl to, jog modeliai pagrinde sukurti raportuoti būseną įvairioms institucijoms pagal tai, pavyzdžiui, skirstančioms resursus.

Trumpai aprašyti modeliai yra apibendrinti 2-oje lentelėje. Patys tinkamiausi tolimesnėje literatūros apžvalgoje yra išnagrinėti detaliau. Šaltiniai, kurie nėra modeliai, naudojami kaip pagalbiniai gilinantis į egzistuojančią metodologiją ir sudarant kibernetinio saugumo procesą.

Modelis	**Leidėjas**	**Komentaras**
C2M2	JAV Energetikos departamentas	Brandos modelis ir įrankis skirtas įsivertinti kibernetinio saugumo gebėjimą.
ES-C2M2	JAV Energetikos departamentas	C2M2 modelis pritaikytas energetikos sektoriui.
ONG-C2M2	JAV Energetikos departamentas	C2M2 modelis pritaikytas naftos ir gamtinių dujų sektoriui.
NICE-CMM	JAV Gynybos departamentas	Apibrėžia tris sritis: procesus ir analitiką, integruotą valdymą, patyrusius praktikus ir technologiją darbo jėgos srities plėtrai.
CERT-RMM	CERT/SEI	Apibrėžia organizacines praktikas tos pačios srities tąsai, saugumui, verslo tęstinumui.
NIST *Cybersecurity Framework*	Nacionalinis standartų ir technologijų institutas, JAV komercijos departamentas	Kibernetinio saugumo struktūrinis modelis rizikos valdymo pagrindu suskirstytas į kategorijas: identifikuoti, apsaugoti, aptikti, atsakyti ir atsistatyti.

2 lentelė. Kibernetinio saugumo vertinimo modeliai ir susiję šaltiniai.

2.2.1.1. C2M2 ir su juo susijusių modelių apžvalga

C2M2 modelis, kuris yra sukurtas ir skirtas organizacijoms padidinti kibernetinio saugumo pajėgumus, yra pasiekiamas viešai ir nemokamai. Organizacijoms, kurios atlieka savęs įsivertinimo testą, yra paruoštas C2M2 pagalbinis įrankis suteikiamas atskirai. Elektros energijos sektoriaus organizacijos ir organizacijos veikiančias naftos ar gamtinių dujų sektoriuje yra nukreipiamos į specializuotus C2M2 modelius, kartu su papildoma nurodomąja informacija.

Nors gali pasirodyti priešingai, tačiau minėtas C2M2 modelis yra išvestinis ir kilęs iš būtent elektros energijos sektoriaus kibernetinio saugumo gebėjimo brandos modelio (ES-C2M2) 1.1 versijos. Konkrečioje versijoje buvo atmesti specifiniai sektoriaus standartai ir terminologija. Tokia iniciatyva buvo pristatyta ir įgyvendinta Baltųjų rūmų institucijos Jungtinėse Amerikos Valstijose kartu su Energetikos ir Saugumo departamentais, taip pat viešojo ir privataus sektoriaus ekspertais.

Kaip teigia Kibernetinio saugumo brandos modelio (C2M2) programos autoriai, modelio pagrindinis sumanymas yra padėti visų tipų organizacijoms įsivertinti ir atlikti teigiamus patobulinimus konkrečioms jau veikiančioms kibernetinio saugumo programoms. C2M2 yra sukurtas pamatuoti tiek programos sofistiką, tiek palaikymą. Modelio akcentas dedamas ties kibernetinio saugumo praktikų, susijusių su informacinių technologijų ir operacinių technologijų turtu bei aplinka, kurioje veikia minėti faktoriai, įgyvendinimu ir valdymu [25].

Modelio tikslas yra kurti logiškai suprantamas ir pamatuojamas politikas, procesus ir procedūras visa tai įtraukiant į organizacijos kibernetinio saugumo paveikslo kūrimą. Modelis suteikia brandos indikatorių lygius, sukurtus identifikuoti organizacijos operacinius gebėjimus ir kibernetinės rizikos valdymą esant įprastoms operacinėms sąlygoms ir krizės metu. Taip pat modelis padeda vykdant kibernetinio saugumo tobulinimo ir vertinimo procesą keliais aspektais, tokiais kaip:

→ organizacijos kibernetinio saugumo galimybių, pajėgumo stiprinimas;

→ galimybė organizacijoms efektyviai ir nuosekliai vertinti, pasiskirsti etaloninį modelį kibernetinio saugumo gebėjimui;

→ terpė dalintis žiniomis, geriausiomis praktikomis ir reikšminga informacija tarp organizacijų, naudojantis tuo kaip gebėjimo tobulinimo galimybe;

→ pagalba organizacijoms prioretizuojant veiksmus ir investicijas siekiant pakelti kibernetinio saugumo lygį;

→ bendra integracija su Nacionalinio standartų ir technologijų instituto (trump. angl. NIST) kibernetinio saugumo struktūra.

Modelis nėra susijęs su jokiais reguliatorių nustatytais reikalavimais. Tai pripažintas ir dokumentuotas ekspertų industrijos geriausių praktikų rinkinys.

Nors modelį autoriai ir apibūdina, kaip tinkantį įvairioms organizacijoms, patys nesigina ir atvirkštinės nuomonės išreiškiančios trūkumus. Priežastys, kodėl modelis netinkamas, yra kelios. Visų pirma, kaip minėta anksčiau modelio karkasas vis dėl to yra specifinė pritaikyta energetikos pramonei versija. Antra, modelio kūrimas ir tobulinimas yra palaikomas JAV administracijos, kontroliuojančios minėtus sektorius, todėl didžiausias suinteresuotumas ir yra kreipiamas būtent į juos, universalų kibernetinio saugumo gebėjimo brandos modelio vertinimą nustumiant į antraplanį vaidmenį, kaip išdavą konkretaus modelio. To pasekoje modelis neprigijo, kaip universalus įsivertinimo įrankis, tačiau turi daug naudingų dalykų tolimesnei analizei ir tikslingam pernaudojimui.

C2M2 siekia suprasti kibernetinio saugumo galimybes lyginant su organizacijos misija dėmesį skiriant praktikoms pagal 10 pagrindinių sričių, kurios prisideda prie bendro kibernetinio saugumo paveikslo organizacijoje. Tos sritys yra:

- ◊ rizikų valdymas;
- ◊ turto, pakeitimų ir konfigūracijos valdymas;
- ◊ tapatybės ir prieigų valdymas;
- ◊ grėsmių ir pažeidžiamumų valdymas;
- ◊ situacijos sąmoningumas;
- ◊ informacijos dalinimasis ir komunikacija;
- ◊ įvykių ir incidentų valdymas, operacijų tęstinumas;
- ◊ tiekimo grandinės ir išorės priklausomybių valdymas;
- ◊ darbo jėgos valdymas;
- ◊ kibernetinio saugumo programos valdymas.

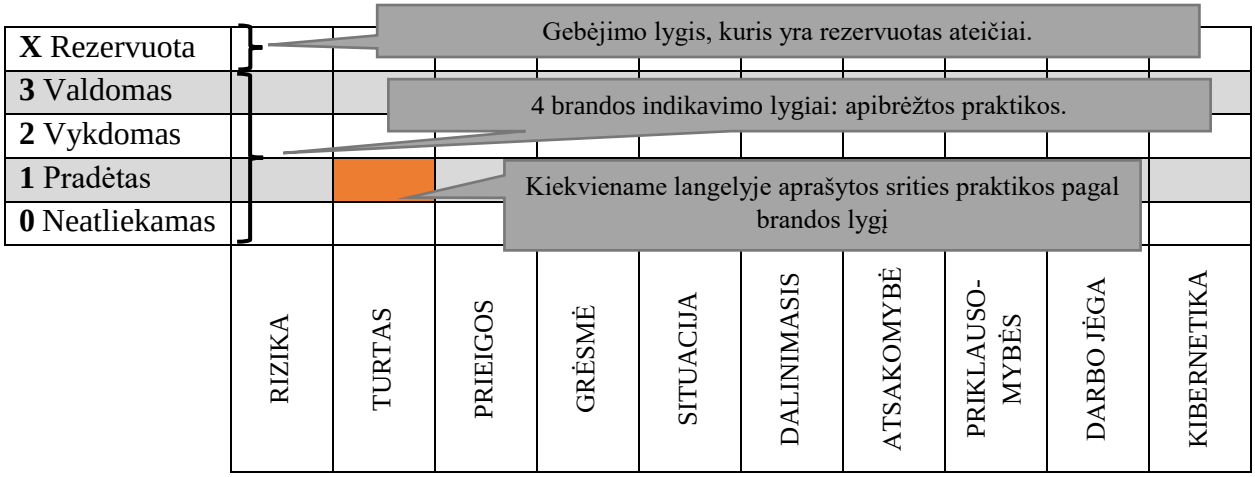
Dalyviai įsivertinant yra prašomi identifikuoti kibernetinio saugumo apibūdinimo, valdymo ir pamatavimo galimybes, taip pat ir veiksmus atliekamus kiekvienoje iš išvardintų sričių.

Įsivertinimas pagal C2M2 reikalauja organizacijos atstovų dalyvavimo. Kibernetinio saugumo komanda turi gebėti diskutuoti apie praktikas kiekviename iš išvardintų punktų, taip pat turėti valdymo lygio suvokimą apie savo funkcijas, departamentų praktikas. Pagrindiniai įsivertinimo dalyviai gali būti šie:

- Vyriausiasis informacijos pareigūnas;
- Vyriausiasis informacijos saugumo pareigūnas;
- Vyriausiasis saugumo pareigūnas;
- Vyriausiasis technologijų pareigūnas;
- Informacinių technologijų direktorius; ir/taip pat
- atsakingi už IT saugumo, IT operacijų valdymą, verslo tęstinumą, kitos susijusios verslo funkcijos.

Kaip žinia yra trijų tipų brandos modeliai, t.y. progresiniai brandos modeliai, brandos gebėjimo modeliai ir hibridiniai modeliai. Būtent toks ir yra C2M2 modelis su savo atmainomis – hibridinis modelis. Tokie modeliai apjungia geriausias progresinių ir gebėjimo brandos modelių sritis. Jie leidžia pamatuoti matavimų evoliuciją ar pasiekimus taip kaip progresiniame modelyje, o taip pat suteikia galimybę pamatuoti gebėjimą ar institucionalizavimą tokiu pačiu tikslumu, kaip tai leidžia padaryti gebėjimo brandos modeliai. Hibridinio modelio lygiai atspindi tiek pasiekimus, tiek gebėjimą.

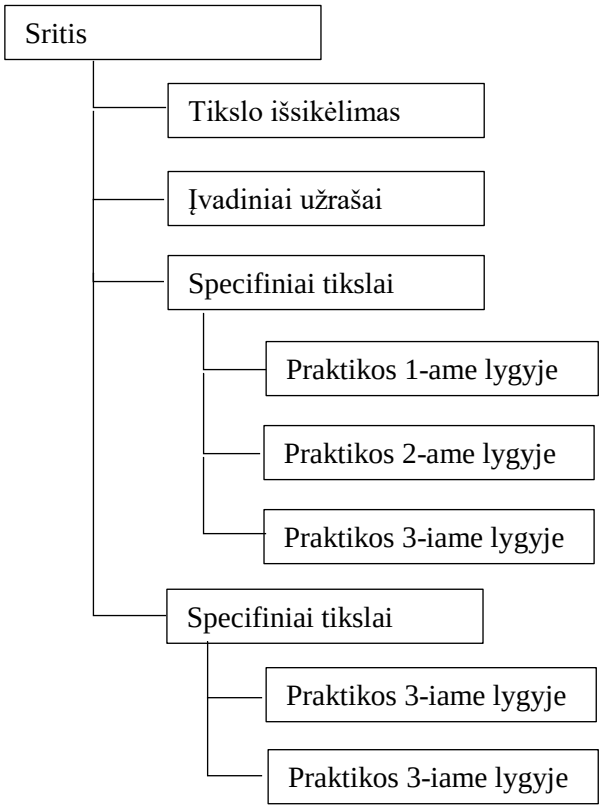
Kaip pavyzdį galima paimti ES-C2M2 modelį, kuris iš C2M2 atšakų yra labiausiai paplitęs, ir tai pavaizduoti grafiškai.



3 lentelė. 10 modelio sričių ir loginis kibernetinio saugumo praktikų grupavimas.

Lygis	Pavadinimas	Aprašymas
MIL0	Neatliekamas	• MIL1 nėra pasiektas pagal nurodytą sritį.
MIL1	Pradėtas	• Praktikos yra pradedamos taikyti, tačiau gali vykti nestruktūrizuotai, pagal poreikį.
MIL2	Vykdomas	• Praktikos yra dokumentuojamos. • Savininkai yra įtraukti. • Adekvatūs resursai yra teikiami palaikyti praktikoms. • Standartai arba gairės yra naudojamos teisingam praktikų įgyvendinimui. • Praktikos yra daugiau pažengusios, užbaigtos negu MIL1 lygyje.
MIL3	Valdomas	• Srities veiklos yra apibrėžtos politikos (ar kitų direktyvų). • Veiklos yra periodiškai peržiūrimos dėl atitikimo politikai. • Atsakomybė ir įgaliojimai praktikoms yra aiškiai priskirti personalo darbuotojams, turintiems pakankamus įgūdžius ir žinias. • Praktikos yra labiau išdirbtos ir pažengusios negu MIL2 lygyje.

4 lentelė. ES-C2M2 modelio panaudojimas.



5 lentelė. ES-C2M2 modelio panaudojimas.

Tokio modelio privalumai yra pagrindinių kompetencijų, o taip pat pajėgumų derinimo, pateikimas lengvesniam vertinimui. Modelis gali būti lengvai pritaikytas technologijų evoliucijai ir praktikoms be gebėjimo matavimo atsisakymo. Įgyvendinimo kaina nėra didelė. Iš kitos pusės, „brandos“ sąvoka nėra tiksliai apibrėžta, o konkrečiau ne taip griežtai kaip įprastuose gebėjimo brandos modeliuose. Kiekvienas lygis gali būti savalaikiškas pagal atributų derinimą su institucionalizavimo ypatybėmis.

Modelio sritys ir jų apipavidalinimas pernaudoti kuriant etaloninį kibernetinio saugumo proceso modelį ir taip pat gryninat kibernetinio saugumo sąvoką. Modelio savybės išsiskiria specifika pramonės sektoriui, todėl pagrinde tik rizikos ir tam tikrų kontrolių sritys tinkamos pernaudoti kuriant universalų modelį.

2.2.1.2. CERT-RMM modelio apžvalga

Pereinant prie kito modelio, tai CERT-RMM pagrindinis dėmesys skiriamas veiklos tęstinumui. Tai apibūdinama kaip organizacijos gebėjimas atsirandantį turtą suvaldyti išlaikant savo susikurtą misiją net ir operacinių trukdžių metu neperžengiant savo galimybių ribos. Išskiriamos pagrindinės naikinimo, gadinimo rizikos grupės, tokios kaip natūrali arba sukurta žmogaus, atsitiktinė arba tyčinė, maža arba didelė, informacinių technologijų ar ne jų, kibernetinė kinetinė.

Pagal šį modelį, saugumas ir verslo tęstinumas yra rizikos valdymo procesas. Tam, kad operacinė rizika būtų valdoma efektyviai, šie procesai turi būti paremti tuo pačiu tikslu. Kitaip sakant, operacinis atsparumas atsiranda dėl veiksmingo operacinės rizikos valdymo.

Rinkoje šis modelis laikomas kaip labiausiai išsami sistema operacinio atsparumo valdymui ir tobulinimui. Modelis būtent ir suteikia gaires tinkamam operacinio atsparumo veiklų kūrimui ir valdymui. Įgalina ir reklamuoja konvergenciją tokių procesų kaip IT atsistatymas po nelaimės, verslo tęstinumas, IT operacijos, kibernetinis saugumas, informacinis saugumas.

CERT-RMM proceso sritys yra šios: prieigų valdymas, turto apipavidalinimas ir valdymas, komunikacija, atitiktis, kontrolių valdymas, dėmesys įmonei, aplinkos kontrolė, išorės priklausomybių valdymas, finansinių resursų valdymas, prieigų valdymas, incidentų valdymas ir kontrolė, bazinių žinių ir informacijos valdymas, matavimai ir analizė, stebėjimas, organizacijos procesų apibrėžimas ir dėmesys procesams, mokymai ir situacijos suvokimo tobulinimas, žmonių valdymas, atsparumo reikalavimų kūrimas ir valdymas, atsparumo techninių sprendimų inžinerija, rizikų valdymas, paslaugų tęstinumas, technologijų valdymas ir pažeidžiamumų valdymas.

CERT-RMM turi keturis gebėjimo lygius įskaitant ir nulinį, kuris yra traktuojamas kaip nepilnas. Pirmame lygyje procesai ir praktikos yra atliekamos, antrame ir trečiame lygiuose atitinkamai valdomos ir aprašytos. Procesai šiuose lygiuose yra pamatuojami, valdomi.

Pavyzdys galėtų būti incidentų valdymo ir kontrolės (IVK) sritis iš visų modelio išvardintų punktų. Tikslas nr. 1 būtų sukurti IVK procesą. Tikslas nr. 2 – aptikti įvykius. Toliau deklaruoti incidentus, atsakyti į incidentus ir atstatyti veiklą, sukurti incidentų reagavimo tobulinimo procesą atitinkamai būtų tikslai nr. 3, 4 ir 5.

Incidentų valdymas pagal gebėjimo brandos modelį atrodytų taip: 0 lygis – organizacija atlieka tam tikras IVK praktikas, 1 lygis – organizacija atlieka visas IVK praktikas, 2 lygis, kai organizacija atlieka IVK praktikas ir planuoja, valdo procesą, jį papildo, apmoko darbuotojus ir pan., o paskutinis 3 lygis – organizacija atlieka viską, kas nusakyta 2-ame lygyje ir turi aprašytą procesą, nuolat kaupia tobulinimui reikalingą informaciją. Verta paminėti, jog institucionalizacija yra kaupiama.

Aptariamo modelio nauda yra tokia, jog modelis pateikia matavimus pagrindinėms kompetencijoms, užtikriną griežtą matavimų pajėgumą, kas yra gebėjimas išlaikyti pagrindines kompetencijas esant stresinėms situacijoms. Modelis pateikia kelią, kaip įgyvendinti matavimus kiekybiniu metodu. Iš kitos pusės, modelį kartais yra sunku suprasti, o tuo labiau pritaikyti, jis brangus įgyvendinti. Branda gali nevirsti tiesioginiais rezultatais. Potencialus neteisingas jausmas dėl pasiekimų: pasiekas aukštą brandos lygis saugumo praktikų srityje nebūtinai reiškia tai, jog organizacija yra „saugi“. Visa tai pernaudojama kuriant etaloninį kibernetinio saugumo proceso modelį.

2.2.1.3. NIST kibernetinio saugumo struktūros modelio apžvalga

Modelio pradinė versija buvo parengta Nacionalinio standartų ir technologijų instituto, kartu įtraukiant ir privatų sektorių, 2014 metų vasarį. Tai buvo atsakas į JAV Prezidento išleistą aktą dėl kritinės infrastruktūros tobulinimo 2013 metais. Į modelio kūrimą buvo įtrauktos lyderiaujančios Amerikos kompanijos. Įsitraukiant ir mokslinei bendruomenei 2018 metų balandžio 16 d. buvo publikuota atnaujinta 1.1 modelio versija. Naujoje versijoje įtraukta papildoma kategorija į identifikavimui priskirtas veiklas – tai tiekėjų grandinės rizikos valdymas. Mokslinis tiriamasis darbas aprodė, jog ši sritis senesnėje modelio versijoje buvo praleista ir trūkstama.

Struktūrinis modelis yra savanoriškas ir konsultacinis arba patariamasis. Jis pagrįstas standartais, gairėmis ir praktikomis. Tinkamiausias organizacijoms valdančioms kritinę infrastruktūrą ir skirtas valdyti ir mažinti kibernetinio saugumo riziką. Be to, tai įrankis palengvinantis komunikaciją organizacijos viduje ir su išorės partneriais ar reguliatoriais. Tai taip pat apima sąmoningumo tobulinimą ir supratimą tarp ir su IT departamentais, planavimo ir operacijų skyriais, aukščiausia vadovybe.

Modelis, kadangi yra patariamojo tipo, turėtų būti adaptuotas ir pritaikytas skirtingiems sektoriams ar atskiroms organizacijoms, kad geriausiai atitiktų rizikas, situacijas ir poreikius.

Organizacijos visada turės ir unikalių rizikų – skirtingos grėsmės, skirtingi pažeidžiamumai, skirtinga tolerancija rizikai – ir kaip organizacijos įgyvendina praktikas, kad pasiektų norimus rezultatus skirsis. Struktūrinis modelis nėra tam tikras klausimynas ar tipiškas modelis tinkantis bet kokiai organizacijai.

Kibernetinio saugumo struktūrinis modelis susideda iš trijų pagrindinių komponentų: branduolio, įgyvendinimo pakopų ir profilių. Modelio branduolys apibūdina norimas pasiekti kibernetinio saugumo veiklas ir rezultatus. Naudojama lengvai suprantama bendra kalba. Branduolys naudojamos organizacijoms siekiant valdyti ir sumažinti kylančias kibernetines rizikas tokiu būdu, kuris leistų praplėsti organizacijoje egzistuojančius kibernetinio saugumo ir rizikų valdymo procesus.

Struktūrinio modelio įgyvendinimo pakopų dalis organizacijoms teikia kontekstą kaip organizacijai valdyti kibernetinio saugumo rizikas. Ši dalis naudojama organizacijoms pasirenkant tinkamą kibernetinio saugumo programos tikslumo lygį ir dažnai naudojama kaip komunikacijos įrankis diskutuojant apie rizikos apetitą, prioretizavimą, biudžetą.

Pakopinė modelio dalis nėra ekvivalenti brandos lygiams. Kertinis šios dalies principas yra apžvelgti vykdomas veiklas iš organizacijos lygio perspektyvos ir nuspręsti, ar dabartinis kibernetinio saugumo rizikos valdymo integracijos lygis yra pakankamas nustatytai misijai, priežiūros tarnybos reikalavimų ir rizikos apetito įgyvendinimui. Progresavimas į aukštesnio lygio pakopą yra rekomenduojamas tada, kai toks pasikeitimas sumažintų kibernetinio saugumo riziką ir būtų efektyvus kainos atžvilgiu.

Struktūrinio modelio profiliai naudojami kaip struktūrinio modelio ir organizacijos reikalavimų ir tikslų, rizikos apetito ir resursų, skiriamų numatytiems rezultatams pagal modelį pasiekti, suvienodinimas. Pirminis tikslas yra identifikuoti ir prioretizuoti galimybes, kaip patobulinti kibernetinį saugumą organizacijoje [15].

Šis modelis naudojamas kaip pagrindas kuriant sisteminį ir nuoseklų požiūrį į kibernetinio saugumo procesą. Medžiaga taip pat naudinga identifikuojant ir atskiriant kibernetinio saugumo procesus nuo informacinio saugumo procesų, vertinant jų sąryšį. Modelio specifika yra eliminuojama kūrimo metu.

2.2.2. Gebėjimo vertinimo ir susijusių modelių panaudojimas

Esamų kibernetinio saugumo brandos gebėjimo modelių analizė atskleidžia, jog modeliai yra komplikuoti siekiant juos įgyvendinti, brangūs laiko ir kainos resursų atžvilgiu, o organizacijos procesai įgyvendinimo atveju turės būti ženkliai keičiami. Kaip bebūtų, reguliatorių ar tam tikrų specifinių sektorių inicijuoti struktūriniai modeliai aprašyti literatūros apžvalgoje remiasi jų

savanorišku panaudojimu įvairiose konkrečiose srityse ir teikia pagrindo analizei, kaip šių modelių adaptacija galėtų būti efektyviai panaudota ir pritaikyta universaliai aplinkai [26].

Siekiant esamus susijusius modelius panaudoti naujo universalaus modelio kūrimui, reikalinga išsiaiškinti kylančias problemas. Everett M. Roggers (1983) aiškina, kad didelės organizacijos, tokios kaip pavyzdžiui savivaldybė ar valstybė, gali tapti vangiomis inovacijų taikyme konkrečiose ūkio šakose. Inovacijų teorija taip pat identifikuoja penkis faktorius, kurie paveikia prisitaikymą: (1) santykinis privalumas (t.y., vertė, kurią teikia inovacija dėl pasirinkto konkretaus metodo); (2) suderinamumas (kaip lengvai inovacija įsilieja į kasdieninę dabartinę rutiną); (3) paprastumas (t.y., ar inovacija yra sudėtinga naudotis); (4) patikrinamumas (kaip lengva išbandyti konkrečią inovaciją be įsipareigojimų); (5) pastebimumas (t.y., kokia matoma tarp bendruomenės narių yra inovacija) [16]. Atsižvelgiant į šiuos penkis veiksnius ir taikytinas kategorijas, keletas jų, pavyzdžiui susijusių su motyvacija ir galimybėmis, turi būti paskirta skatinti priimti kibernetinio saugumo gebėjimo brandos modelį.

Padidėjęs pažeidžiamumų pastebimumas (5) kokio nors tai rinkos dalyvio gali įtakoti susijusios asociacijos veiklą ir formuoti impulsą pakeitimui ar adaptacijai visoje rinkoje. Panašiai, sustiprėjusios reguliatorinės sistemos ar tam tikra žala padaryta dėl atsiradusių pažeidžiamumų gali formuoti įsipareigojimus vadovybei, kurie taip pat galiausiai atsilieps vykstantiems pokyčiams rinkoje. Kibernetinio saugumo brandos gebėjimo modelių taikymo pasiekiamumas organizacijos darbuotojams gali formuoti paprastumo (3) ir patikrinamumo (4) principus.

3. Kibernetinio saugumo proceso nuo taikomosios praktikos nepriklausomo etaloninio modelio kūrimas

Šį mokslinį tiriamąjį darbą būtų galima suskirstyti į kelias dalis. Pirmiausia nustatomi reikalavimai procesų modeliui. Remiantis mokslinės literatūros apžvalga, sukuriamas kibernetinio saugumo proceso išvestinis modelis. Jo procesai aprašyti tokiais atributais kaip identifikavimas, paskirtis, rezultatai. Šis modelis yra lyginamas ir gretinamas su NIST kibernetinio saugumo struktūros modeliu, taip pat keliais informacinio saugumo procesų modeliais. Visa tai atliekama siekiant tinkamai paruošti medžiagą naujo kibernetinio saugumo proceso etaloninio modelio kūrimui.

Pagrindinis šaltinis proceso modelio reikalavimų nustatymui yra ISO/IEC 33004 programų inžinerijos standartas. Šis standartas pasirinktas kaip pagrindas dėl jo plataus ir įvairiapusiško naudojimo galimybių, kurios jau ne kartą yra įrodytos [17][27]. Proceso modelių pavyzdžiai naudoti praktiniam pritaikymo supratimui.

Kibernetinio saugumo proceso kategorijos ir procesai kurti remiantis geriausiomis praktikomis ir standartais. Dauguma tų praktikų, standartų ar modelių yra specifiniai, pritaikyti vienam ar kitam sektoriui, tačiau didžiausia problema, jog nė vienas jų neadresuoja proceso veiklos, o pagrinde būseną. Dėl to reikalinga agreguoti ir suvienodinti didelį kiekį įvairios ir skirtingos bent kiek susijusios informacijos [26].

3.1. Reikalavimai procesų modelio kūrimui

Proceso modelis yra tos pačios prigimties apjungtų į modelį procesų rinkinys. Taigi, proceso modelis yra tam tikro tipo procesų aprašymas, o procesas yra pagrindinė modelio sudedamoji dalis. Tas pats proceso modelis yra naudojamas pakartotinai vertinti daug organizacijų. Viena iš galimų proceso modelio panaudojimo galimybių yra apibūdinti, kaip dalykai turėtų/galėtų būti įgyvendinami lyginant su modelįo procesus indikuojačiomis geriausiomis praktikomis. Proceso modelis yra abstraktus veiklos procesų apibendrinimas.

Proceso modeliai gali būti skirstomi pagal tikslus į:

- Apibūdinančius;
  - Seka kas esminio iš tikrųjų vyksta veiklos proceso metu;
  - Žvelgiama iš menamos išorės stebėtojo perspektyvos, kuris vertina proceso atlikimą ir nustato būtinus patobulinimus, kurie leistų procesą vykdyti efektyviau ir veiksmingiau.
- Nurodančius;
  - Apibūdina norimą pasiekti procesą ir kas turi būti atlikta;

- Nustato taisykles, gaires ir elgesio modelius kurie, jeigu sekami, turėtų nuvesti iki užsibrėžtos proceso atlikimo stadijos. Galima variacija tikslumu.

- Aiškinamuosius.
  - Suteikia paaiškinimus apie procesų loginį pagrindą;
  - Tiria ir vertina keletą galimų veiksmų kursų pagrįstų racionaliais argumentais.

Šiuo konkrečiu atveju pagal tikslą labiausiai tinkamas apibūdinantis modelis. Jo pagrindu bus kuriamas kibernetinio saugumo modelis.

Gilinantis iš organizacijos perspektyvos, proceso modeliavimas apima verslo architektūros proceso aspektus ir veda į viską apimančią organizacijos architektūrą. Ryšiai tarp verslo procesų visų likusių organizacijos sistemų, duomenų, organizacinės struktūros, strategijos ir t.t. kontekste kuria didesnius gebėjimus analizuojant ir planuojant pakeitimus. Vienas realaus pasaulio pavyzdys yra organizacijų sujungimas ar įsigijimas; procesų supratimas iki detalių abiejose organizacijose taip leidžia vadovybei identifikuoti persidengimus ir sklandžiai susijungti [24].

Procesų modeliai taip pat klasifikuojami pagal aprėptį ir suderinamumą. Pagal aprėptį šiuo atveju tikslinis modelis būtų orientuotas į veiklą [18]: susijęs veiklų rinkinys skirtas konkrečiam produkto apibrėžimui; iš dalies sutvarkytų žingsnių rinkinys, sukurtas pasiekti tikslą. Kiti tipai, tai į produktą orientuotas modelis, į sprendimą, kontekstą, strategiją plačiau nėra aprašomi.

Pagal suderinamumą procesai skirstomi į strateginius, taktinius ir įgyvendinimo [19]. Tinkamiausias šiuo atveju taktinis priskyrimas. Jis padeda įgyvendinti planą ir labiau koncentruotas į aktualaus plano pasiekimo taktinius veiksmus nei į patį plano kūrimą.

Žvelgiant plačiau ir į būsimus uždavinius, reikia pasigilinti į gebėjimo vertinimo modelius. Gebėjimo modelių ištakos prasideda programinės įrangos kūrimo industrijoje, kur modeliai tarnavo kaip rekomenduojamų patobulinimų organizacijoms, norinčioms pakelti programinės įrangos kūrimo proceso brandą, rinkinys [2]. Įprastai, gebėjimo brandos modelis turi du komponentus: (a) matavimo ir objekto reikšmes, kurios nurodo nuoseklaus kūrimo būdą, paremtą hierarchine progresija, ir (b) kriterijus (tokius kaip būsenos, procesai ar aplikacijos tikslai) skirtus pamatuoti objektų gebėjimą. Apjungti šie komponentai suteikia brandos lygių seką objekto klasėms. Kitais žodžiais tariant, gebėjimo brandos modelis atstoja numatomą, pageidaujamą arba tipišką tų objektų pokyčio kelią nusakytą diskrečiais etapais [5].

Kadangi tai yra informatikos disciplinos mokslo darbas, pagrindinis reikalavimų šaltinis šiame darbe yra ISO/IEC 33004 programų inžinerijos standartas. Detalūs šio standarto reikalavimai taikomi pačio kibernetinio saugumo proceso etaloninio modelio kūrimo ir tobulinimo metu.

3.2. Procesų modelių ir susijusių šaltinių palyginimas

Apibrėžus reikalavimus procesų modelio kūrimui ir išnagrinėjus mokslinę literatūrą, susijusius šaltinius, reikalinga sudaryti etaloninį kibernetinio saugumo proceso modelį tolimesniam jo tobulinimui. Etaloninis modelis kuriamas dviem etapais. Pirmuoju etapu analizės pagrindu sumaketuojamas išvestinis modelis iš esamų kibernetinio saugumo specifinių brandos gebėjimo modelių. Pastebėta, jog toks išvestinis modelis turi trūkumų ir sunku identifikuoti specifinius tik kibernetiniam saugumui būdingus procesus – jie dalinai persidengia su informacinio saugumo valdymo sistemos procesais pagal ISO 2700x. To pasekoje atliktas modelių palyginimas. Į palyginimą įtraukti informacinio saugumo procesus apjungiantys modeliai, kad būtų galima išskirti tik kibernetiniam saugumui būdingus ar dalinai persidengiančius procesus, įtraukas sukurtas išvestinis kibernetinio saugumo proceso modelis ir NIST kibernetinio saugumo struktūrinis modelis kaip standartas kibernetinio saugumo veikloms.

Išvestinis kibernetinio saugumo proceso modelis, nors ir sukurtas pagal geriausius rinkoje egzistuojančius ir ištobulintus modelius, turi netikslumų ir trūkumų. Vienas jų yra neišbaigti organizacinės ir pagalbinės kategorijos procesai. Šis trūkumas analizuojamas sekančioje darbo dalyje apie integraciją su ISO/IEC 33071 (toliau - *Enterprise* SPICE).

Kitas trūkumas yra nuoseklumo kibernetinio saugumo inžineriniuose procesuose stygius. Šiam trūkumui pašalinti buvo svarstytos dvi galimybės remiantis geriausiomis praktikomis: kategorizuoti procesus pagal įsilaužimo eigą ir sudėlioti kibernetinio saugumo procesus iš įsilaužėlio perspektyvos arba pernaudoti NIST siūlomą rizikos valdymu pagrįstą modelio kategorizavimą. Pastarasis būdas ir buvo pasirinktas kaip pagrindas tolimesniam etaloninio modelio procesų kategorizavimui ir vystymui. Kuriant etaloninį kibernetinio saugumo proceso modelį procesai buvo kategorizuoti atitinkamai išgryninant specifines kibernetinio saugumo specifines sritis.

6-oje lentelėje pavaizduotas aprašytas išvestinis kibernetinio saugumo procesų modelis. Modelis sukurtas įtraukiant literatūros apžvalgoje išskirtas kibernetinio saugumo praktikas ir atitinka Enterprise SPICE metodologiją. Modelis turi tris procesų kategorijas. Detalus išvestinio kibernetinio saugumo proceso modelio aprašymas pateikiamas darbo priede Nr. 2.

Organizacinių procesų kategorija įgalina kibernetinio saugumo inžinerinius procesus, užtikrina atitinkamus resursus, jų teisingą valdymą ir tinkamą kompetenciją, taip pat sąmoningumo ir žinių bazės ugdymą. Visa tai leidžia inžineriniams procesams veikti. Inžinerinių procesų kategorija sudaryta iš pirminių procesų reikalingų kibernetinio saugumo proceso įgalinimui ir vykdymui organizacijoje. Pagalbinių procesų kategorija skiriama tam, kad kibernetinio saugumo funkcijos įgalinimas būtų pakankamas ir užtikrintas.

Organizaciniai procesai	Inžineriniai procesai	Pagalbiniai procesai
Strategijos ir politikų valdymas	Reikalavimų valdymas	Atitikties testavimas
IT turto valdymas	Perimetro apsauga	Auditavimas ir neatitikimų stebėjimas
Rizikos valdymo programa	Privilegijų naudojimo valdymas	Paskyrų prieigų priežiūra
Resursų užtikrinimas	Konfigūracijos valdymas	Įsilaužimų imitavimas
Mokymų programos valdymas	Pakeitimų kontrolė	Duomenų panaudojimo valdymas
Kultūros puoselėjimas	Tinklo apsauga	
	Atnaujinimų, kodų pataisymų valdymas ir diegimas	
	Aplikacijų saugumas	
	Galutinių įrenginių apsauga	
	Kriptografijos paslaugos	
	Saugumo būsenos stebėjimas ir kontrolė	
	Pasirengimas kibernetiniams įsilaužimams	

6 lentelė. Išvestinis universalus kibernetinio saugumo procesų modelis.

Analizuojant gauto modelio procesus, pastebėta, jog pagal literatūros apžvalgoje išvestą kibernetinio saugumo apibrėžimą, ne visi procesai patenka į modelio rėmus. Kai kurie procesai sutampa su ISO 33072 informacinio saugumo proceso gebėjimo brandos vertinimo modelio išskirtais procesais, kai kurie jų persidengia, o kai kurie lieka specifiniai. Siekiant sumažinti galimų neatitikimų kiekį, į palyginimą įtraukti ir ISO 2700x informacinio saugumo valdymo sistemos (ISVS) išskirti procesai. Pasirodo, kad net lyginant ISO 2700x ISVS procesus su ISO 33072 standartu, yra neatitikimų ir tam tikrų specifinių procesų.

Visa ši procesų aibė sugretinta su NIST kibernetinio saugumo struktūros modelio veiklomis ir išvestinio kibernetinio saugumo proceso modeliu. Procesai kategorizuoti ir atrinkti tinkami sudaryti etaloniniam kibernetinio saugumo proceso modeliui. Minėtų modelių palyginimas ir kategorizavimas apipavidalinti 7-oje lentelėje.

	NIST *Cybersecurity Framework*[2]	**Kibernetinio saugumo proceso išvestinis modelis[3]**	**ISMS *Core Processes*[4] (ISO 2700x)**	**ISO 33072[5]**	**Komentaras etaloninio modelio sudarymui**
Identifika	[IDN] Turto valdymas	[ORG] IT turto valdymas		[ORG] Turto valdymas	Procesas įtraukiamas ir specializuojamas kibernetinio saugumo disciplinai.
				[ORG] Įrangos valdymas	

[2] Trumpinių naudojamų NIST modelyje pilni pavadinimai: [IDN] – identifikavimas; [APS] – apsaugojimas; [APT] – aptikimas; [RGV] – reagavimas; [ATS] – atsistatymas.

[3] Trumpinių naudojamų Kibernetinio saugumo proceso etaloniniame modelyje pilni pavadinimai: [ORG] – organizaciniai procesai; [INZ] – inžineriniai procesai; [PAG] – pagalbiniai procesai.

[4] Trumpinių naudojamų ISO 2700x pilni pavadinimai: [VLD] – valdymo procesai; [PAP] – papildantys procesai; visi kiti laikomi kaip pagrindiniai procesai pagal standarto apibrėžimus.

[5] Trumpinių naudojamų ISO 33072 pilni pavadinimai: [ORG] – organizaciniai procesai, [VLD] – bendri integruoti valdymo procesai; [TEC] – techniniai procesai.

	[IDN] Verslo aplinka		Informacinio saugumo klientų santykių valdymo procesas	[ORG] Infrastruktūra ir darbo aplinka	Procesas nėra įtraukiamas kaip specifinis kibernetinio saugumo sričiai ir padengtas SPICE modelio organizacinių procesų kategorija.
	[IDN] Valdymas	[ORG] Strategijos ir politikų valdymas	[VLD] Informacinio saugumo valdymo procesas		Procesas nėra įtraukiamas kaip specifinis kibernetinio saugumo sričiai ir padengtas SPICE modelio organizacinių procesų kategorija.
				[VLD] Neatitikties valdymas	
		[INZ] Reikalavimų valdymas	Reikalavimų valdymo procesas	[TEC] Paslaugų reikalavimai	
	[IDN] Rizikos vertinimas	[ORG] Rizikos valdymo programa	Informacijos saugumo rizikos vertinimo procesas		Procesas įtraukiamas ir specializuojamas kibernetinio saugumo disciplinai.
	[IDN] Rizikos valdymo strategija		Informacinio saugumo rizikos švelninimo procesas		Procesas nėra įtraukiamas, nes padengtas SPICE standarto organizacinių procesų kategorija.
	[IDN] Tiekimo grandinės rizikos valdymas			[ORG] Tiekėjų valdymas	Procesas nėra įtraukiamas, nes padengtas SPICE standarto organizacinių procesų kategorija.
Apsaugojimas	[APS] Tapatybės ir prieigų valdymas	[PAG] Paskyrų prieigų priežiūra			Procesas įtraukiamas į etaloninį modelį. Procesas praplečiamas pagal atitinkamus išvestinio modelio procesus.
		[INZ] Privilegijų naudojimo valdymas			
	[APS] Sąmoningumas ir mokymai	[ORG] Mokymų programos valdymas	Procesas, skirtas užtikrinti reikiamą sąmoningumą ir kompetencijas		Procesas nėra įtraukiamas, nes padengtas SPICE standarto pagalbinių procesų kategorija.
		[ORG] Kultūros puoselėjimas			
	[APS] Duomenų saugumas	[INZ] Kriptografijos paslaugos			Procesas įtraukiamas.
		[PAG] Duomenų panaudojamumo valdymas			
	[APS] Informacijos apsaugos procesas ir procedūros	[INZ] Pakeitimų kontrolė	Informacijos saugumo pakeitimų valdymo procesas	[TEC] Pakeitimų valdymas	Procesas į modelį nėra įtraukiamas kaip informacinio saugumo srities procesas.
		[INZ] Konfigūracijos valdymas	[PAP] Konfigūracijos valdymo procesas	[TEC] Konfigūracijos valdymas	
	[APS] Priežiūra (palaikymas)				Įtraukiamas kaip svarbus kibernetinio saugumo objektas – organizacijos resursų prieiga nuotoliniu būdu.
	[APS] Apsaugančios technologijos	[INZ] Aplikacijų saugumas			Procesas pilnai patenka į kibernetinio saugumo srities apibrėžimą. Neturi jokių susietų informacinio saugumo procesų.
		[INZ] Galutinių įrenginių apsauga			
		[INZ] Perimetro apsauga			
Aptikimas	[APT] Anomalijos ir įvykiai	[INZ] Tinklo apsauga			Procesas pilnai patenka į kibernetinio saugumo srities apibrėžimą. Neturi jokių susietų informacinio saugumo procesų.

	[APT] Nuolatinis saugumo stebėjimas	[INZ] Atnaujinimų, kodų pataisymų valdymas ir diegimas			Procesas pilnai patenka į kibernetinio saugumo srities apibrėžimą. Neturi jokių susietų informacinio saugumo procesų.
		[INZ] Saugumo būsenos stebėjimas ir kontrolė			
	[APT] Aptikimo procesas				Procesas pilnai patenka į kibernetinio saugumo srities apibrėžimą. Neturi jokių susietų informacinio saugumo procesų.
Reagavimas	[RGV] Reagavimo planavimas	[INZ] Pasirengimas kibernetiniams įsilaužimams	Informacinio saugumo incidentų valdymo procesas	[TEC] Incidentų valdymas	Procesas įtraukiamas ir specializuojamas kibernetinio saugumo disciplinai.
				[TEC] Paslaugų tęstinumo valdymas	
				[TEC] Paslaugų pasiekiamumo valdymas	
	[RGV] Komunikacijos		Komunikacijos procesas	[VLD] Komunikacijos valdymas	Procesas įtraukiamas ir specializuojamas kibernetinio saugumo disciplinai.
	[RGV] Analizė				Procesas įtraukiamas į etaloninį modelį.
	[RGV] Sušvelninimas				Procesas įtraukiamas į etaloninį modelį.
	[RGV] Tobulinimai	[PAG] Atitikties testavimas			Procesas įtraukiamas į etaloninį modelį ir praplečiamas.
		[PAG] Įsilaužimų imitavimas			
Atstatymas	[ATS] Atsistatymo planavimas			[TEC] Techninis duomenų saugojimas ir atkūrimas	Procesas specializuojamas ir įtraukiamas.
	[ATS] Tobulinimai		Informacijos saugumo tobulinimo procesas	[VLD] Tobulinimas	Proceso rezultatai apjungiami su reagavimo kategorijos tobulinimų procesu kaip persidengiantys.
	[ATS] Komunikacijos				Proceso rezultatai apjungiami su reagavimo kategorijos komunikacijų procesu kaip persidengiantys.
Nepatenkantys į kategorijas procesai			[VLD] ISMS planavimo procesas	[VLD] Vadovybės peržiūra	
		[ORG] Resursų užtikrinimas	Resursų valdymo procesas	[VLD] Žmogiškųjų išteklių valdymas	
				[ORG] Žmogiškųjų išteklių įdarbinimo valdymas	
			Dokumentacijos ir įrašų kontrolės valdymo procesas	[VLD] Dokumentacijos valdymas	
			Veiklos vertinimo procesas	[VLD] Veiklos vertinimas	
		[PAG] Auditavimas ir neatitikimų stebėjimas	Vidaus audito procesas	[VLD] Vidaus auditas	Procesas yra padengiamas SPICE pagalbinių procesų kategorija.
				[VLD] Operacinis planavimas	
				[VLD] Operacinis įgyvendinimas ir kontrolė	

				[TEC] Pajėgumų valdymas	
				[TEC] Produkto/paslaugos paleidimas	

7 lentelė. Modelių procesų palyginimas ir sugretinimas.

Sukurto išvestinio kibernetinio saugumo proceso vertinimo modelio sugretinimas su NIST standarte identifikuotais procesais padėjo įvesti nuoseklumą modeliui. Palyginimas su informacinio saugumo procesais leido suprasti skirtumą ir identifikuoti nesusijusius procesus, taip pat specializuoti persidengiančius procesus. Toliau kibernetinio saugumo proceso modelis nagrinėjamas plačiau kitais kampais.

3.3. Integracija su *Enterprise* SPICE

Kuriant išvestinį kibernetinio saugumo proceso modelį ir atliekant įvairių modelių palyginimą paaiškėjo, jog identifikuoti organizacinės ir pagalbinės kategorijų procesai tik dalinai padengia procesus išskirtus patvirtintuose standartuose. Atliktas vertinimas nustatyti sąryšį tarp išskirtų kategorijose procesų ir apibūdinti integraciją su *Enterprise* SPICE standartu. Šis sugretinimas pavaizduotas 8-oje lentelėje.

Organizaciniai procesai		
NIST *Cybersecurity Framework*	Kibernetinio saugumo proceso išvestinis modelis	*Enterprise* SPICE
[IDN] Valdymas	[ORG] Strategijos ir politikų valdymas	Įmonės valdymas
		Investicijų valdymas
	[ORG] Resursų užtikrinimas	Žmogiškųjų išteklių valdymas
		Įmonės architektūra
[IDN] Verslo aplinka		Verslo ryšių valdymas
[IDN] Tiekimo grandinės rizikos valdymas		Tiekėjų sutarčių valdymas
		Projektų valdymas
[IDN] Rizikos valdymo strategija	[ORG] Rizikos valdymo programa	Rizikos valdymas

Pagalbiniai procesai		
Enterprise SPICE	Kibernetinio saugumo proceso išvestinis modelis	NIST *Cybersecurity Framework*
Alternatyvų analizė		
Vertinimas ir analizė	[PAG] Įsilaužimų imitavimas	
	[PAG] Projektų ir pakeitimų saugumo vertinimas	
Kokybės užtikrinimas ir valdymas	[PAG] Auditavimas ir neatitikimų stebėjimas	
	[PAG] Atitikties testavimas	
	[PAG] Paskyrų prieigų peržiūra	
Informacijos valdymas	[PAG] Duomenų panaudojamumo valdymas	
Žinių valdymas		
Mokymai	[ORG] Mokymų programos valdymas	[APS] Sąmoningumas ir mokymai
Tyrimai ir inovacijos		
Darbo aplinka	[ORG] Kultūros puoselėjimas	
Proceso aprašymas		
Proceso tobulinimas		

8 lentelė. Organizacinių ir pagalbinių procesų integracija su Enterprise SPICE (ISO/IEC 33071 standartu).

Iš palyginimo matyti, jog visi kibernetinio saugumo proceso etaloninio modelio sudarymui išskirti organizaciniai procesai yra padengiami *Enterprise* SPICE organizaciniais arba pagalbiniais procesais. Visi išskirti pagalbiniai procesai yra padengiami *Enterprise* SPICE pagalbinių procesų kategorija.

Pavyzdžiui, *Enterprise* SPICE modelio organizacinės kategorijos procesas rizikų valdymas apima tiek išvestinio modelio rizikos valdymo programos procesą, tiek NIST standarto identifikacinės grupės procesą – rizikos valdymo strategija. Šių procesų rezultatai, nors skirtingai aprašyti ir išdėstyti, turi tą pačią reikšmę. Kitas pavyzdys, tai *Enterprise* SPICE standarte įtrauktas pagalbinis mokymų procesas. Šio proceso rezultatai abstraktesniame lygyje yra tokie patys kaip išvestinio modelio ar NIST veiklos rezultatai.

Iš kitos pusės, išskirti procesai yra ne tik padengiami *Enterprise* SPICE standarto organizacinių ir pagalbinių procesų kategorijomis, tačiau juos praplečia. Tokio organizacinės kategorijos proceso kaip projektų valdymas nėra išskirta nei išvestiniame modelyje, nei NIST standarte. Svarbūs pagalbiniai procesai. *Enterprise* SPICE standarto pagalbiniai procesai rezultatų atžvilgiu padengia pavienius išvestinio modelio pagalbinius procesus, taip pat klaidingai kategorizuotus organizacinius procesus.

Enterprise SPICE yra pripažintas standartas ISO/IEC 33074, todėl juo remiamasi kaip pagrindu ir to pasekoje kuriamas Enterprise SPICE modelio praplėtimas kibernetinio saugumo sričiai.

3.4. Kibernetinio saugumo proceso etaloninis modelis

Atliekant mokslinį tyrimą, literatūros apžvalga papildyta kitais moksliniais literatūros šaltiniais, plačiau ir įvairiais rakursais aprašančiais proceso modelio kūrimą ir kibernetinio saugumo discipliną. Remiantis palyginimu, procesai grupuoti ir atrinkti, taip sudarant įvesties medžiagą kibernetinio saugumo proceso kūrimui.

Remiantis medžiaga ir atsižvelgiant į programų inžinerijos ISO 33004 standarto reikalavimus, sukurtas kibernetinio saugumo proceso etaloninio modelis procesų identifikatorius pateikiamas 9-oje lentelėje. Modelis sudarytas iš trijų proceso kategorijų – organizacinių, inžinerinių ir pagalbinių procesų. Inžineriniai procesai sugrupuoti atskiromis dalinėmis rizikos valdymo pagrindu grįstomis kategorijomis suteikiančiomis kibernetinio saugumo procesui nuoseklumą ir tvarką. Kiekvienai dalinei kategorijai priskirti atitinkami kibernetinio saugumo procesai pagal grupavimą.

Organizaciniai procesai (*Enterprise* SPICE)	Inžineriniai procesai		Pagalbiniai procesai (*Enterprise* SPICE)
Įmonės valdymas	Identifikavimas	IT turto valdymas	Alternatyvų analizė
Investicijų valdymas		Kibernetinio saugumo rizikos vertinimas	Vertinimas ir analizė
Žmogiškųjų išteklių valdymas	Apsaugojimas	Tapatybės ir prieigų valdymas	Kokybės užtikrinimas ir valdymas
Įmonės architektūra		Duomenų saugumas	Informacijos valdymas
Verslo ryšių valdymas		Priežiūra (palaikymas)	Žinių valdymas
Tiekėjų sutarčių valdymas		Apsaugančios technologijos	Mokymai
Projektų valdymas	Aptikimas	Anomalijos ir įvykiai	Tyrimai ir inovacijos
Rizikos valdymas		Nuolatinis saugumo stebėjimas	Darbo aplinka
		Aptikimo procesas	Proceso aprašymas
	Reagavimas	Reagavimo planavimas	Proceso tobulinimas
		Komunikacijos	
		Analizė	
		Sušvelninimas	
		Tobulinimas	
	Atsistatymas	Atsistatymo planavimas	

9 lentelė. Kibernetinio saugumo proceso modelis – Enterprise SPICE plėtinys.

Organizaciniai ir pagalbiniai procesai detaliau aprašomi *Enterprise* SPICE standarte, o inžineriniai procesai aprašomi tolimesniame skyriuje sudarant kibernetinio saugumo proceso gebėjimo vertinimo modelį. Sekančiame etape modelis validuojamas. Šis kibernetinio saugumo proceso vertinimo modelis atitinka išsikeltą universalumo reikalavimą, taip pat apibrėžtą kibernetinio saugumo sąvoką.

4. Kibernetinio saugumo proceso gebėjimo vertinimo modelis

Kibernetinio saugumo proceso gebėjimo vertinimo modelis yra sukurtas remiantis programų inžinerijos standarto ISO/IEC 33004 reikalavimais. Pagal tai, proceso tikslas ir rezultatai turi būti apibrėžti kaip sėkmingo proceso įgyvendinimo siekimas ir būti trumpi, aiškūs. Taip pat pagal minimą standartą, proceso brandos gebėjimo vertinimo modelis apibrėžiamas grupe rodiklių, kurie atitinkamai apibūdina tikslą ir rezultatus, ir tai nurodo proceso atributų pasiekimus.

Modelis sudarytas iš trijų procesų kategorijų – inžinerinių procesų, pagalbinių procesų ir organizacinių procesų. Inžineriniai procesai yra aprašyti šiame skyriuje ir taikomi kaip plėtinys *Enterprise* SPICE standartui kibernetinio saugumo srityje. Pagalbiniai procesai ir organizaciniai procesai yra detaliai aprašyti *Enterprise* SPICE standarte.

4.3. Inžineriniai procesai

Inžineriniai procesai yra specifiniai kibernetinio saugumo sričiai. Procesai suskirstyti į penkias dalines kategorijas: identifikavimo, apsaugojimo, aptikimo, reagavimo ir atsistatymo. Kiekvienas atskiras procesas aprašytas identifikatoriumi – trimis pirmosiomis kategorijos pavadinimo raidėmis, trimis pirmosiomis dalinės kategorijos raidėmis atskirtomis tašku ir skaitine reikšme, pavadinimu, paskirtimi, rezultatais, bazinėmis praktikomis.

3.2.1. Identifikavimo procesų dalinė kategorija

Identifikavimo dalinė kategorija apibrėžia organizacijos supratimo kaip valdyti kibernetinio saugumo riziką sistemoms, žmonėms, turtui, duomenims, ugdymą. Procesai šioje kategorijoje yra esminiai efektyviam kibernetinio saugumo valdymui. Organizacijai, norinčiai efektyviai siekti užsibrėžto tikslo kibernetinio saugumo srityje, reikia suprasti organizaciją supančią aplinką, valdyti resursus palaikančius kritinius verslo procesus, o visa tai vykdyti paraleliai su rizikos valdymo strategija ir organizacijos misija. Šios kategorijos procesai yra IT turto valdymas ir kibernetinio saugumo rizikos vertinimas.

3.2.1.1. IT turto valdymas

	IT turto valdymas	
INZ.IDN01	Paskirtis	Rezultatai
	Inventorizuoti duomenis, prietaisus, sistemas, kurios reikalingos pasiekti verslo iškeltiems tikslams, saugumo priemonių poreikio išsiaiškinimui ir užtikrinimui.	1. Fiziniai prietaisai organizacijoje yra suinventorizuojamos. 2. Sistemos organizacijoje yra suinventorizuotos. 3. Programinė įranga organizacijoje yra suinventorizuota. 4. Organizacijos komunikacijos srautai yra dokumentuojami. 5. Išorinės informacijos sistemos yra kataloguojamos. 6. Resursai (pavyzdžiui, techninė įranga, duomenys, laikas, programinė įranga) yra prioretizuojami pagal vertę verslui.

		7. Turto valdymui naudojami automatizuoti įrankiai. 8. Kibernetinio saugumo atsakomybės yra apibrėžtos.
	Bazinės praktikos	
	BP.1: Inventorizuoti fizinius prietaisus organizacijoje. [Rezultatas: 1] BP.2: Inventorizuoti organizacijos sistemas. [Rezultatas: 2] BP.3: Inventorizuoti organizacijos turimą programinę įrangą. [Rezultatas: 3] BP.4: Dokumentuoti organizacijos duomenų srautus. [Rezultatas: 4] BP.5: Kataloguoti išorines informacijos sistemas. [Rezultatas: 5] BP.6: Prioretizuoti įvairius organizacijos resursus pagal jų sukuriamą vertę verslui. [Rezultatas: 6] BP.7: Naudoti automatizavimą turto valdymui. [Rezultatas: 7] BP.8: Apibrėžti kibernetini o saugumo roles ir atsakomybes organizacijoje. [Rezultatas: 8]	

3.2.1.2. Kibernetinio saugumo rizikos vertinimas

INŽ.IDN02	Kibernetinio saugumo rizikos vertinimas	
	Paskirtis	Rezultatai
	Valdyti ir prioretizuoti organizacijos resursus ginantis nuo grėsmių valdant pažeidžiamumus ir atsižvelgiant į kylančias grėsmes.	1. Turto pažeidžiamumai yra identifikuoti. 2. Kibernetinio saugumo žvalgybos informacija iš informacijos dalinimosi platformų yra naudojama rizikos vertinime. 3. Grėsmės, tiek vidinės, tiek išorinės yra identifikuotos. 4. Potencialus poveikis verslui yra identifikuotas. 5. Naudojamasi rizikos valdymo metodologija. 6. Rizikos švelninimo priemonės yra prioretizuojamos. 7. Vadovybė yra įtraukta į rizikų vertinimą.
	Bazinės praktikos	
	BP.1: Identifikuoti pažeidžiamumus turtui. [Rezultatas: 1] BP.2: Naudoti kibernetinio saugumo žvalgybos informaciją, gautą iš įvairių informacijos dalinimosi platformų, rizikos vertinime. [Rezultatas: 2] BP.3: Identifikuoti išorines ir vidines grėsmes rizikos vertinimui. [Rezultatas: 3] BP.4: Identifikuoti potencialų poveikį verslui. Jį išmatuoti. [Rezultatas: 4] BP.5: Naudotis patvirtinta rizikos valdymo metodologija. [Rezultatas: 5] BP.6: Prioretizuoti rizikos švelninimo priemones. [Rezultatas: 6] BP.7: Įtraukti vadovybę į rizikų vertinimą. [Rezultatas: 7]	

3.2.2. Apsaugojimo procesų dalinė kategorija

Apsaugojimo procesų kategorija apibrėžia tinkamų saugumo priemonių kūrimą ir įgyvendinimą, kad kritiniai organizacijos procesai nebūtų sutrikdyti. Ši procesų kategorija sudaro galimybę užkirsti kelią arba sumažinti potencialaus kibernetinio saugumo įvykio poveikį. Kategorijos procesai yra tokie: tapatybės ir prieigų valdymas, duomenų saugumas, priežiūra, apsaugančios technologijos.

3.2.2.1. Tapatybės ir prieigų valdymas

IN	Tapatybės ir prieigų valdymas	
	Paskirtis	Rezultatai

	Pasiekti fizinius ir loginius įrenginius leisti tik autorizuotiems vartotojams, procesams ir įrenginiams.	1. Autorizuotų įrenginių, vartotojų ir procesų kredencialai yra valdomi. 2. Fizinė prieiga prie turto yra valdoma. 3. Nuotolinė prieiga yra valdoma. 4. Prieigos teisės yra valdomos. 5. Tinklo vientisumas yra apsaugotas. 6. Tapatybės yra priskirtos kredencialams. 7. Vartotojai, įrenginiai ir kitas turtas yra autentifikuoti. 8. Privilegijų naudojimas yra ribojamas pagal poreikį.
	Bazinės praktikos	
	BP.1: Autorizuoti įrenginius, vartotojus ir procesus. [Rezultatas: 1] BP.2: Valdyti autorizuotų įrenginių, vartotojų, procesų kredencialus. [Rezultatas: 1] BP.3: Valdyti fizinę prieigą prie organizacijos turto. [Rezultatas: 2] BP.4: Valdyti nuotolinę prieigą prie organizacijos turto. [Rezultatas: 3] BP.5: Valdyti prieigos teises organizacijoje. [Rezultatas: 4] BP.6: Apsaugoti tinklo vientisumą. [Rezultatas: 5] BP.7: Priskirti tapatybes kredencialams. [Rezultatas: 6] BP.8: Autentifikuoti vartotojus, įrenginius ir kitą turtą. [Rezultatas: 7] BP.9: Riboti privilegijų naudojimą pagal poreikį. [Rezultatas: 8]	

3.2.2.2. Duomenų saugumas

INZ.APS02	Duomenų saugumas	
	Paskirtis	Rezultatai
	Nuosekliai valdyti informaciją ir duomenis apsaugant konfidencialumą, vientisumą ir pasiekiamumą pagal organizacijos rizikos strategiją.	1. Organizacijos duomenys yra apsaugoti. 2. Perkeliami duomenys yra apsaugoti. 3. Turtas yra valdomas formaliai viso gyvavimo ciklo metu. 4. Adekvatus pajėgumų lygis yra palaikomas siekiant užtikrinti pasiekiamumą. 5. Apsauga nuo duomenų nutekinimo yra įgyvendinama. 6. Vientisumo patikrinimo mechanizmai yra naudojami. 7. Plėtros ir bandymo aplinkos yra atskirtos nuo produkcinės aplinkos. 8. Vientisumo patikrinimo mechanizmai yra naudojami patikrinti techninės įrangos vientisumą.
	Bazinės praktikos	
	BP.1: Apsaugoti laikomus duomenų talpyklose organizacijos duomenis. [Rezultatas: 1] BP.2: Apsaugoti perkeliamus duomenis. [Rezultatas: 2] BP.3: Valdyti turtą formaliai, dokumentuoti viso gyvavimo ciklo metu. [Rezultatas: 3] BP.4: Palaikyti adekvatų pajėgumų lygį, kuris leistų užtikrinti pasiekiamumą. [Rezultatas: 4] BP.5: Įgyvendinti apsaugą nuo duomenų nutekinimo. [Rezultatas: 5] BP.6: Naudoti vientisumo patikrinimo mechanizmus. [Rezultatas: 6] BP.7: Atskirti plėtros ir bandymo aplinkas nuo produkcinės aplinkos. [Rezultatas: 7] BP.8: Naudoti vientisumo patikrinimo mechanizmus patikrinti techninės įrangos vientisumą. [Rezultatas: 8]	

3.2.2.3. Priežiūra (palaikymas)

IN	Priežiūra (palaikymas)	
	Paskirtis	Rezultatai

	Informacinėms ir pramonės kontrolės sistemoms atlikti palaikymo ir remonto darbus pagal apibrėžtą politiką ir atitinkamas procedūras.	1. Patvirtinti įrankiai yra naudojami organizacijos turto priežiūrai. 2. Organizacijos turto priežiūra yra dokumentuojama. 3. Priežiūra nuotoliniu būdu yra patvirtinamas. 4. Priežiūra nuotoliniu būdu yra dokumentuojama. 5. Autorizuotos prieigos naudojamos priežiūrai nuotoliniu būdu.
	Bazinės praktikos	
	BP.1: Naudoti patvirtintus įrankius organizacijos turto priežiūrai. [Rezultatas: 1] BP.2: Dokumentuoti organizacijos turto priežiūrą. [Rezultatas: 2] BP.3: Patvirtinti priežiūrą nuotoliniu būdu. [Rezultatas: 3] BP.4: Dokumentuoti priežiūrą, atliekamą nuotoliniu būdu. [Rezultatas: 4] BP.5: Naudoti autorizuotas prieigas priežiūrai nuotoliniu būdu. [Rezultatas: 5]	

3.2.2.4. Apsaugančios technologijos

INZ.APS04	Apsaugančios technologijos	
	Paskirtis	Rezultatai
	Pagal galiojančias politikas, procedūras ir susitarimus techniniai saugumo sprendimai yra naudojami siekiant užtikrinti sistemų ir turto saugumą ir apsaugą.	1. Audito įvykiai yra renkami. 2. Audito įvykių įrašai yra peržiūrimi. 3. Keičiamos laikmenos yra valdomos. 4. Tik reikiamos funkcijos yra naudojamos sistemose pagal konfigūraciją. 5. Komunikacijos tinklai yra apsaugoti. 6. Mechanizmai leidžiantys įgyvendinti atsparumo reikalavimus yra valdomi.
	Bazinės praktikos	
	BP.1: Rinkti audito įvykius iš sistemų. [Rezultatas: 1] BP.2: Peržiūrėti audito įvykių įrašus. [Rezultatas: 2] BP.3: Valdyti keičiamąsias laikmenas. [Rezultatas: 3] BP.4: Naudoti tik reikiamas funkcijas sistemose pagal konfigūraciją. [Rezultatas: 4] BP.5: Apsaugoti komunikacijos tinklus. [Rezultatas: 5] BP.6: Valdyti mechanizmus, kurie leidžia įgyvendinti atsparumo reikalavimus. [Rezultatas: 6]	

3.2.3. Aptikimo procesų dalinė kategorija

Aptikimo procesų kategorija skirta kurti ir įgyvendinti tinkamus procesus, kad būtų galima aptikti kibernetinio saugumo įvykį. Sekantys procesai įgalina laiko atžvilgiu efektyvų kibernetinio saugumo įvykių aptikimą. Tai anomalijos ir įvykiai, nuolatinis saugumo stebėjimas, aptikimo procesas.

3.2.3.1. Anomalijos ir įvykiai

INZ.APT01	Anomalijos ir įvykiai	
	Paskirtis	Rezultatai
	Aptikti anomalijas ir suprasti potencialų įvykių poveikį.	1. Bazinis tinklo operacijų saugumo lygis yra valdomas. 2. Aptikti incidentai yra analizuojami siekiant suprasti atakos principus.

		3. Įvykių duomenys yra koreliuojami iš įvairių šaltinių. 4. Įvykių poveikis yra apskaičiuojamas. 5. Incidentų aliarmo ribos yra nustatytos.
	Bazinės praktikos	
	BP.1: Valdyti bazinį tinklo operacijų saugumo lygį. [Rezultatas: 1] BP.2: Aptikti incidentus. [Rezultatas: 2] BP.3: Analizuoti aptiktus incidentus siekiant suprasti atakos principus. [Rezultatas: 2] BP.4: Koreliuoti įvykių duomenis iš įvairių sistemų. [Rezultatas: 3] BP.5: Apskaičiuoti įvykių poveikį. [Rezultatas: 4] BP.6: Nustatyti incidentų aliarmo ribas siekiant išvengti per didelio netikro pavojaus signalų. [Rezultatas: 5]	

3.2.3.2. Nuolatinis saugumo stebėjimas

INZ.APT02	Nuolatinis saugumo stebėjimas	
	Paskirtis	Rezultatai
	Identifikuoti kibernetinio saugumo incidentus informacinėse sistemose ir kituose įrenginiuose, ir patvirtinti apsaugos priemonių efektyvumą.	1. Tinklas yra stebimas siekiant aptikti potencialius kibernetinio saugumo įvykius. 2. Fizinė aplinka yra stebima siekiant aptikti potencialius kibernetinio saugumo incidentus. 3. Personalo veikla yra stebima siekiant aptikti potencialius saugumo incidentus. 4. Kenkėjiškas kodas yra aptinkamas. 5. Neautorizuotas mobilus kodas yra aptinkamas. 6. Išorės paslaugų tiekėjų veiklą yra stebima siekiant aptikti potencialius kibernetinio saugumo incidentus. 7. Neautorizuoto personalo, prisijungimų, įrenginių, programinės įrangos stebėjimas yra atliekamas. 8. Pažeidžiamumų skanavimai yra atliekami.
	Bazinės praktikos	
	BP.1: Stebėti tinklą siekiant aptikti potencialius kibernetinio saugumo įvykius. [Rezultatas: 1] BP.2: Stebėti fizinę aplinką siekiant aptikti potencialius kibernetinio saugumo incidentus. [Rezultatas: 2] BP.3: Stebėti personalo veiklą siekiant aptikti potencialius kibernetinio saugumo incidentus. [Rezultatas: 3] BP.4: Aptikti kenkėjišką kodą. [Rezultatas: 4] BP.5: Aptikti neautorizuotą mobilų kodą. [Rezultatas: 5] BP.6: Stebėti išorės tiekėjų paslaugų veiklą siekiant aptikti potencialius kibernetinio saugumo incidentus. [Rezultatas: 6] BP.7: Atlikti neautorizuoto personalo, prisijungimų, įrenginių, programinės įrangos stebėjimą. [Rezultatas: 7] BP.8: Atlikti pažeidžiamumų skanavimus. [Rezultatas: 8]	

3.2.3.3. Aptikimo procesas

INZ.APT03	Aptikimo procesas	
	Paskirtis	Rezultatai
	Palaikyti ir tikrinti anomalių įvykių aptikimo	1. Atsakomybės aptikimo procese yra tinkamai apibrėžtos. 2. Aptikimo veiklos suderinamos su kitais taikomais reikalavimais.

	sąmoningumą ir gebėjimą.	3. Aptikimo procesas yra testuojamas. 4. Įvykių aptikimo informacija yra komunikuojama. 5. Aptikimo procesai yra nuolatos tobulinami.
	Bazinės praktikos	
	BP.1: Tinkamai apibrėžti roles ir atsakomybes aptikimo procese. [Rezultatas: 1] BP.2: Suderinti aptikimo veiklas su kitais galiojančiais ir taikomais reikalavimais. [Rezultatas: 2] BP.3: Testuoti ir išbandyti aptikimo procesą. [Rezultatas: 3] BP.4: Komunikuoti įvykių aptikimo informaciją organizacijos viduje ir išorėje. [Rezultatas: 4] BP.5: Nuolatos tobulinti aptikimo procesus. [Rezultatas: 5]	

3.2.4. Reagavimo procesų dalinė kategorija

Ši procesų kategorija skirta sukurti ir įgyvendinti procesus leidžiančius imtis atitinkamų ir reikiamų veiksmų aptikus kibernetinio saugumo incidentą. Procesai leidžia suvaldyti tokių incidentų poveikį. Jie yra: reagavimo planavimas, komunikacijos, analizė, sušvelninimas, tobulinimas.

3.2.4.1. Reagavimo planavimas

INZ.RGV01	Reagavimo planavimas	
	Paskirtis	Rezultatai
	Užtikrinti tinkamą atsaką kibernetinio saugumo incidentams.	1. Kibernetinio incidento suvaldymo planas yra aprašytas. 2. Reagavimo planas yra vykdomas incidento metu. 3. Reagavimo planas yra vykdomas suvaldžius incidentą. 4. Incidentų statistika yra naudojama rizikų vertinimui.
	Bazinės praktikos	
	BP.1: Aprašyti kibernetinio incidento suvaldymo planą. [Rezultatas: 1] BP.2: Vykdyti reagavimo planą kibernetinio incidento metu. [Rezultatas: 2] BP.3: Vykdyti reagavimo planą suvaldžius kibernetinį incidentą. [Rezultatas: 3] BP.4: Naudoti incidentų statistiką rizikų vertinimui. [Rezultatas: 4]	

3.2.4.2. Komunikacijos

INZ.RGV02	Komunikacijos	
	Paskirtis	Rezultatai
	Koordinuoti reagavimo veiklas su vidaus ir išorės atsakingais.	1. Personalas žino savo operacinius veiksmus, kai atsakas yra reikalingas. 2. Incidentai yra raportuojami pagal nustatytus kriterijus. 3. Informacija yra dalinamasi pagal sudarytus planus. 4. Koordinavimas tarp atsakingų vyksta pagal nustatytus planus. 5. Siekiant platesnio kibernetinio saugumo sąmoningumo informacija apie incidentus yra dalinamasi su išore.
	Bazinės praktikos	
	BP.1: Personalui žinoti savo operacinius veiksmus vykstant ir įvykus kibernetiniam incidentui. [Rezultatas: 1]	

	BP.2: Raportuoti kibernetinio saugumo incidentus pagal nustatytus kriterijus. [Rezultatas: 2] BP.3: Dalintis informacija apie kibernetinio saugumo įvykius pagal nustatytus planus. [Rezultatas: 3] BP.4: Koordinuoti kibernetinio saugumo incidentų informaciją tarp atsakingų asmenų ar institucijų pagal nustatytus planus. [Rezultatas: 4] BP.5: Dalintis informacija apie kibernetinio saugumo incidentus su išore siekiant platesnio kibernetinio saugumo sąmoningumo. [Rezultatas: 5]

3.2.4.3. Analizė

INZ.RGV03	Analizė	
	Paskirtis	Rezultatai
	Užtikrinti efektyvų reagavimą į incidentus ir papildyti susijusius veiklas.	1. Pranešimai iš aptikimo sistemų yra tiriami. 2. Incidento poveikis yra suprantamas. 3. Ekspertizė yra atliekama. 4. Incidentai yra kategorizuojami pagal apibrėžtus planus. 5. Pažeidžiamumai sužinomi iš išorės šaltinių yra tikrinami.
	Bazinės praktikos.	
	BP.1: Tirti pranešimus iš aptikimo sistemų. [Rezultatas: 1] BP.2: Suprasti incidento poveikį ir tuo pasinaudoti atliekant tolimesnius veiksmus. [Rezultatas: 2] BP.3: Atlikti incidentų ekspertizę. [Rezultatas: 3] BP.4: Kategorizuoti incidentus pagal apibrėžtus planus ir kriterijus. [Rezultatas: 4] BP.5: Tikrinti pažeidžiamumus sužinomus iš išorės atitinkamų šaltinių. [Rezultatas: 5]	

3.2.4.4. Sušvelninimas

INZ.RGV04	Sušvelninimas	
	Paskirtis	Rezultatai
	Užkirsti įvykio sklaidos tikimybę, sušvelninti patirtus nuostolius ir išspręsti incidentą.	1. Incidentų informacija yra renkama. 2. Incidentai yra valdomi. 3. Naujai identifikuoti pažeidimai yra valdomi rizikų pagrindu.
	Bazinės praktikos	
	BP.1: Rinkti detalią informaciją apie incidentus ir ją panaudoti analizei. [Rezultatas: 1] BP.2: Valdyti incidentus. [Rezultatas: 2] BP.3: Valdyti naujai identifikuotus pažeidžiamumus rizikų valdymo pagrindu. [Rezultatas: 3]	

3.2.4.5. Tobulinimas

INZ.RGV05	Tobulinimas	
	Paskirtis	Rezultatai
	Pritaikyti esamų ir istorinių incidentų informaciją tobulinti incidentų valdymo veiklas.	1. Iš incidentų yra mokomasi. 2. Incidentų valdymo strategija yra atnaujinama.
	Bazinės praktikos	

	BP.1: Mokytis iš incidentų ir pagal tai atnaujinti procesus, sistemas ar planus. [Rezultatas: 1] BP.2: Atnaujinti incidentų valdymo strategiją pagal vykstančius incidentus ir reikiamas priemones ar resursus tiems incidentams suvaldyti. [Rezultatas: 2]

3.2.5. Atsistatymo procesų dalinė kategorija

Atstatymo kategorijos proceso pagalba kuriamas ir įgyvendinamas planas sukurti atsparumą ir atstatyti bet kokias reikiamas funkcijas ar paslaugas, kurios buvo paveiktos kibernetinio saugumo incidento metu. Tai turi būti atliekama laikui efektyviu atžvilgiu. Šios kategorijos procesas yra atstatymo planavimas.

3.2.5.1. Atsistatymo planavimas

INZ.ATS01	Atsistatymo planavimas	
	Paskirtis	Rezultatai
	Užtikrinti turto ar sistemų atsistatymą po kibernetinio saugumo incidentų pagal apibrėžtas procedūras ir procesus.	1. Atsistatymo planas yra naudojamas kibernetinės atakos metu. 2. Atsistatymo planas yra naudojamas pasibaigus kibernetinei atakai.
	Bazinės praktikos	
	BP.1: Naudoti atsistatymo planą kibernetinio saugumo incidento metu. [Rezultatas: 1] BP.2: Naudoti atsistatymo planą kibernetinei atakai pasibaigus. [Rezultatas: 2]	

Toliau šis sukurtas modelis darbe yra vadinamas CyberSPICE terminu.

5. Kibernetinio saugumo proceso gebėjimo vertinimo modelio validavimas

Išsiaiškinti sukurto CyberSPICE modelio praplėtimo kibernetinio saugumo procesui validumą, reikalinga proceso brandos gebėjimo vertinimo modelį pritaikyti organizacijoje. Šiam tikslui pasirinkta organizacija, kurios pavadinimas dėl konfidencialumo sutarimo nėra minimas. Toliau tekste ši organizacija, naudota modelio adekvatumo tvirtinimui, yra vadinama tiesiog organizacija.

Organizacijos veiklos pobūdis ir aplinka verčia skirti atitinkamą dėmesį kibernetinio saugumo sričiai. Organizacija turi dedikuotus resursus vystančius kibernetinį saugumą ir išmanančius šią sritį. Šie specialistai dalyvauja apklausoje ir tai daro organizaciją tinkamu objektu modelio teisingumo patikrinimui.

Organizacija vertinama pagal sudaryto kibernetinio saugumo proceso gebėjimo brandos modelio inžinerinių procesų kategoriją, kuri praplečia *Enterprise* SPICE standartą kibernetinio saugumo srityje. Organizacija nebus vertinama pagal organizacinius ir pagalbinius procesus apibrėžtus standarte, nes jie ir taip yra patvirtinti. Vertinimas aprašytas darbo validavimo dalyje.

Nustačius organizacijos kibernetinio saugumo proceso esamą gebėjimo profilį, jai bus sudarytas tikslinis gebėjimo profilis ir atitinkamai pagerintas organizacijos kibernetinio saugumo proceso sudarytas veiklos modelis pagal tikslinį gebėjimo profilį. Tai aprašyta rezultatų apibendrinimo dalyje.

5.3. Validavimo aprašymas

Organizacijos kibernetinio saugumo proceso modelio inžineriniai procesai vertinami pagal tai, kokia apimtimi praktika yra vykdoma organizacijoje. Atsižvelgiama į bendrąsias praktikas, bendruosius resursus ir darbo produktus procesų atlikimo atributams. Tai reiškia, jog yra naudojami resursai atlikti užsibrėžtus proceso gerųjų praktikų tikslus. Taip pat egzistuoja darbo produktai, kurie gali būti panaudoti kaip procesų išvesties įrodymai. Vertinama pagal žemiau pateiktą skalę atitinkančią ISO/IEC 33020 standartą.

Praktika yra:		
F	Pilnai vykdoma	86-100 proc.
L	Vykdoma	85-51 proc.
P	Dalinai vykdoma	16-50 proc.
N	Nevykdoma	0-15 proc.

10 lentelė. Praktikų vertinimo skalė.

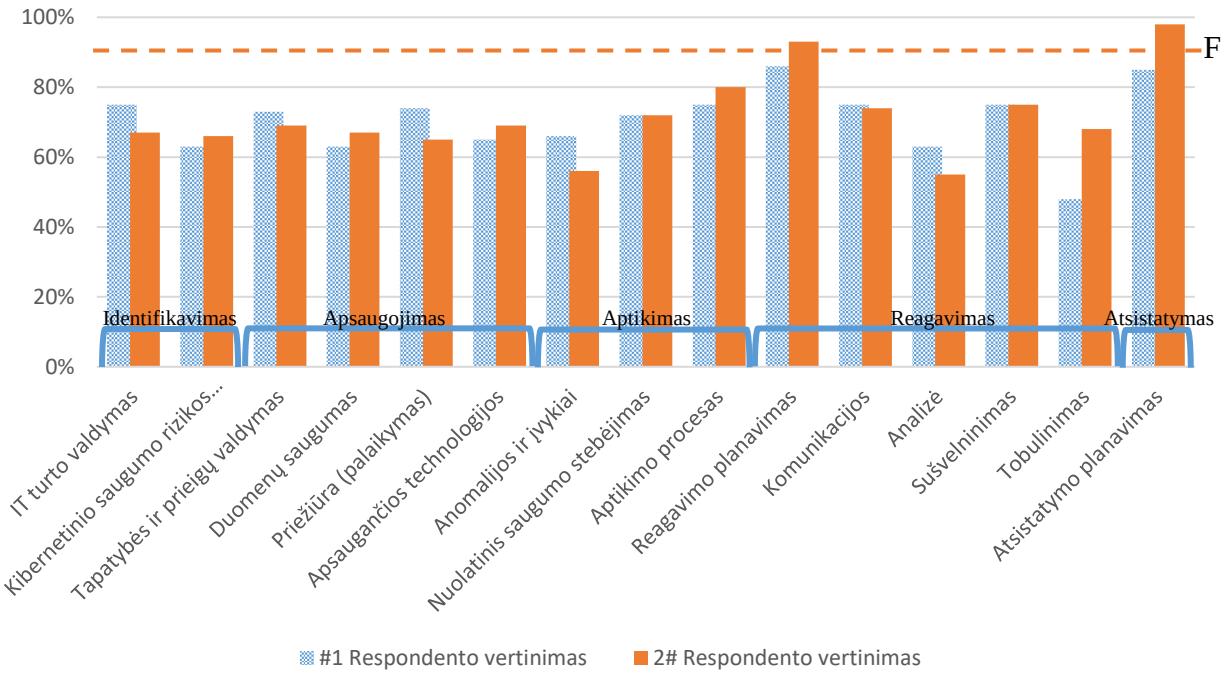
Kiekviena praktika yra vertinama dviejų tiesiogiai nesusijusių, tačiau dirbančių kibernetinio saugumo srityje, specialistų. Praktika vertinama procentine išraiška ir graduojama pagal atitinkamai apibrėžtos skalės ribas. Kiekvienas modelio procesas yra apibendrinamas pagal respondento kokybinį vertinimą. Organizacijoje buvo apklausiami du kibernetinio saugumo

specialistai – vienas jų vadovaujantis techninei komandai, o kitas kibernetinio saugumo valdymo ir procesų komandai. Respondentų vertinimai buvo palyginti ir išvestas jų aritmetinis vidurkis. Detalus vertinimas pateikiamas darbo priede Nr. 3, o apibendrinamoji lentelėje žemiau Nr. 11.

Proceso dalinė kategorija	Procesas	Proceso atributas 1.1.	Lygis	Vertinimas
Identifikavimas	IT turto valdymas	L	1	71 %
	Kibernetinio saugumo rizikos vertinimas	L	1	65 %
Apsaugojimas	Tapatybės ir prieigų valdymas	L	1	71 %
	Duomenų saugumas	L	1	65 %
	Priežiūra (palaikymas)	L	1	70 %
	Apsaugančios technologijos	L	1	67 %
Aptikimas	Anomalijos ir įvykiai	L	1	61 %
	Nuolatinis saugumo stebėjimas	L	1	72 %
	Aptikimo procesas	L	1	78 %
Reagavimas	Reagavimo planavimas	F	1	90 %
	Komunikacijos	L	1	75 %
	Analizė	L	1	59 %
	Sušvelninimas	L	1	75 %
	Tobulinimas	L	1	58 %
Atsistatymas	Atsistatymo planavimas	F	1	92 %

11 lentelė. Įvertinti organizacijos procesai

Iš rezultatų matyti, jog apie 13 proc. procesų organizacijoje yra vykdomi pilnai, o visi likę yra vykdomi. Dviejų respondentų atsakymų vidurkių skirtumo vidurkis yra 6,4 proc., kas leidžia teigti, jog sukurto CyberSPICE – *Enterprise* SPICE praplėtimo kibernetiniam saugumui – modelis yra suprantamas ir pakankamai aiškus. Respondentų atsakymų vidurkiai kiekvienam procesui pateikti 5 pav. Tik kelios praktikos buvo nevykdomos arba dalinai vykdomos. Dviejų praktikų vidurkiai rodo pilnai vykdomą praktiką, todėl šios yra vertinamos antru lygiu.



5 pav. Respondentų atsakymų palyginimas.

Reagavimo planavimo ir atsistatymo planavimo procesai, kurie yra pilnai vykdomi pirmu lygiu (vykdomi procesai), yra vertinami antru lygiu (valdomi procesai) pagal ISO/IEC 33020 standartą. Tai reiškia, jog prieš tai aprašyti ir pilnai atliekami procesai yra įgyvendinami juos valdant (planuojant, stebint, pritaikant). Darbo produktai yra tinkamai sukurti, kontroliuojami ir palaikomi.

Procesą vertinant antru lygiu atsižvelgiama į atlikimo valdymo atributą. Tai proceso atlikimo valdymo matas ISO/IEC 33020 standarte identifikuojamas kaip proceso atributas (PA) 2.1. Šio atributo pilno įgyvendinimo rezultatai yra tokie:

a) proceso vykdymo tikslai yra nustatyti;

b) proceso atlikimas yra planuojamas ir stebimas;

c) proceso atlikimas yra pritaikomas, kad pasiektų užbrėžtus tikslus;

d) atsakomybės ir įgaliojimai proceso atlikimui yra apibrėžti, priskirti ir iškomunikuoti;

e) resursai ir reikiama informacija siekiant atlikti procesą yra identifikuoti, prieinami, priskirti ir naudojami;

f) sąsajos su įtrauktomis pusėmis yra valdomos, kad būtų užtikrinta efektyvi komunikacija ir aiškus atsakomybių priskyrimas.

Bendrosios praktikos PA 2.1 yra detaliau aprašytos nurodytame standarte. Respondentų detalus vertinimas pateikiamas priede *Nr. 4. Pilnai vykdomų procesų vertinimas antru lygiu*. Pagal šį vertinimą galima daryti išvadą, jog procesas INZ.RGV01 pavadintas reagavimo planavimu vertinant jį antru lygiu ir atsižvelgiant į abiejų respondentų atsakymų vidurkį yra įvertintas 53 proc. ir pagal vertinimo skalę tai reiškia, jog proceso valdymas yra vykdomas (L).

Procesas INZ.ATS01 – atsistatymo planavimas – vertinant jį antru lygiu ir atsižvelgiant į abiejų respondentų atsakymų vidurkį yra įvertintas 55 proc. ir pagal vertinimo skalę tai reiškia, jog proceso valdymas taip pat yra vykdomas (L).

Kitas proceso atributas 2.2 yra darbo produkto valdymo atributas. Pasitelkiant jį matuojamas gaunamų darbo produktų apimties tinkamas valdymas. Pilnai įgyvendinamo atributo rezultatai yra šie:

a) reikalavimai proceso darbo produktui yra apibrėžti;

b) reikalavimai dokumentacijai ir darbo produktų kontrolei yra apibrėžti;

c) darbo produktai yra tinkamai identifikuoti, dokumentuoti ir kontroliuojami;

d) darbo produktai yra peržiūrimi pagal planuojamus susitarimus ir pritaikomi atitikti reikalavimus.

Bendrosios praktikos PA 2.2 yra detaliau aprašytos minimame standarte ir priede Nr. 4 kartu su respondentų vertinimu. Apibendrinant proceso produktų darbo vertinimas tiek reagavimo planavimo procese, tiek atsistatymo planavimo procese yra dalinai vykdomas (P) atitinkamai

respondentams vidutiniškai įvertinus 23 proc. ir 37 proc. Apibendrintas vertinimo rezultatas pateikiamas 12 lentelėje.

Proceso dalinė kategorija	Procesas	Organizacijos vertinimas pirmu lygiu	Organizacijos vertinimas antru lygiu	
			PA 2.1.	PA 2.2.
Reagavimas	Reagavimo planavimas	F	L	P
Atsistatymas	Atsistatymo planavimas	F	L	P

12 lentelė. Antru lygiu įvertinti organizacijos procesai.

Remiantis procesų atributų vertinimo rezultatais ir ISO/IEC 33020 standarto reikalavimais, galima daryti išvadą, jog procesai reagavimo planavimas ir atsistatymo planavimas nepasiekia antro lygio, tačiau lieka įvertinti pirmu lygiu.

5.4. Rezultatų apibendrinimas

Atlikus tyrimą buvo prieita išvados, jog modelyje nėra nereikalingų ar neadekvačių inžinerinių kibernetinio saugumo procesų. Jie visi buvo vykdomi organizacijoje ir pripažinti kaip reikalingi kibernetinio saugumo vadovų. Taip pat atliekant apklausą nebuvo pastebėta jokių perteklinių praktikų, kurios nepakliūtų į kibernetinio saugumo sritį ar būtų atliekamos tik kitų sričių, kaip pavyzdžiui, informacinio saugumo, ekspertų.

Nors organizacijos kibernetinio saugumo proceso gebėjimas įvertintas aukščiau nei vidurkis, o kai kur praktikos pilnai vykdomos, yra ką tobulinti. Iš vertinimo matyti, jog nors su incidentais ir yra susitvarkoma, jų suvaldymui pasiruošta, tačiau pats incidentų aptikimo procesas ir susiję aptikimo procesai yra vykdomi tik dalinai. Beveik nevykdomas audito įrašų peržiūrėjimo procesas, nors jie ir yra renkami.

Iš esmės tobulinant kiekvienos praktikos gebėjimą organizacijos kibernetinio saugumo proceso lygis būtų padidintas iki pilnai vykdomo. Tam tikroms sritims, kurios dabar atliekamos dalinai, turėtų būti skirtas atitinkamas dėmesys ir resursai prioretizuoti šioje srityje. Įvertinus pilnai vykdomus procesus matyti, jog pirmiausia turi būti stiprinamas darbo produktų valdomumas norint pasiekti aukštesnį brandos lygį.

6. Išvados ir apibendrinimas

Kibernetinio saugumo proceso gebėjimo vertinimo modelis šiame darbe yra sukurtas ir validuotas. Modelis sukurtas kaip pripažinto programų inžinerijos standarto *Enterprise* SPICE plėtinys kibernetinio saugumo procesui. Darbo eigoje buvo įrodyta, jog iš kitų geriausių kibernetinio saugumo praktikų išskirti organizacinės ir pagalbinės kategorijos procesai yra pilnai ir kokybiškai padengiami *Enterprise* SPICE standarte aprašytais organizaciniais ir pagalbiniais procesais. Būtent inžinerinių procesų kategorija yra praplėsta kibernetinio saugumo procesais.

Šie procesai yra suskirstyti į penkias grupes paremtas rizikų valdymu ir išlaikant proceso nuoseklumą. Grupės yra: identifikavimas, apsauga, aptikimas, reagavimas, atsistatymas. Kiekvienai grupei priskirti atitinkami kibernetinio saugumo procesai sudarant bendrą ir viską apjungiantį kibernetinio saugumo proceso gebėjimo vertinimo modelį. Kibernetinio saugumo procesai yra atrinkti iš geriausių praktikų veiklų. Specifikos atsisakyta kiek įmanoma modelį sudarant universalų ir nepriklausomą. Kiekvienas procesas aprašytas paskirtimi, rezultatais ir bazinėmis praktikomis.

Modelis validuotas remiantis realia egzistuojančia organizacija skiriančia didelį dėmesį kibernetinio saugumo sričiai. Apklausti du kibernetinio saugumo srities vadovai atsakingi už techninį ir procedūrinį šios srities įgyvendinimą organizacijoje. Tyrimas parodė, jog modelis neturi perteklinių procesų, atskleidžia realią organizacijos situaciją kibernetinio saugumo srityje ir identifikuoja spragas. Modelis leidžia organizacijai identifikuoti dalinai vykdomas veiklas ir jas tobulinti prioretizavimo pagrindu.

Kibernetinio saugumo proceso gebėjimo vertinimo modelis kaip plėtinys programų inžinerijos *Enterprise* SPICE standarto užpildo universalaus modelio trūkumą šioje specifinėje srityje. To pasekoje kuriamas pagrindas struktūrizuotam kibernetinio saugumo vertinimui procesų kūrimo ir valdymo srityje. Modelis yra nepriklausomas ir sukurtas mokslo pagrindais.

Detali medžiaga ir informacija apie modelio sudarymą ir patį modelį gali būti pateikta atskiru prašymu darbo autoriaus elektroninio pašto adresu tomas.martinkenas@mif.stud.vu.lt .

7. Naudotos literatūros sąrašas

[1] ISACA, CISM Review Manual 14th Edition. ISBN 978-1-60420-369-1, p. 139-260.

[2] The maturity of maturity model research: A systematic mapping study [interaktyvus]. Roy Wendler, Information and Software Technology, Volume 54, Issue 12, December 2012, Pages 1317–1339 [žiūrėta 2017 m. rugsėjo 17 d.]. Prieiga per internetą: <http://www.sciencedirect.com/science/article/pii/S0950584912001334>.

[3] Walter Miron, Kevin Muita. Capability Maturity Models for Providers of Critical Infrastructure [interaktyvus]. October 2014 [žiūrėta 2016 m. spalio 1 d.]. Prieiga per internetą: <https://timreview.ca/sites/default/files/article_PDF/MironMuita_TIMReview_October2014.pdf>.

[4] Information technology – Process assessment – Requirements for process reference, process assessment and maturity models, ISO/IEC 33004:2014, 2014-02-24.

[5] Maturity Models in Business Process Management [interaktyvus]. Maximilian Röglinger, Jens Pöppelbuß, Jörg Becker in: Business Process Management Journal 18 (2012) 2 [žiūrėta 2017 m. gegužės 3 d.]. Prieiga per internetą: <http://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/352/wi-352.pdf>.

[6] Re-Engineering IT Internal Controls: Applying Capability Maturity Models to the Evaluation of IT Controls [interaktyvus]. Conference Paper · February 2006 [žiūrėta 2017 m. rugsėjo 15 d.]. Prieiga per internetą: <https://www.researchgate.net/publication/4216252_Re-Engineering_IT_Internal_Controls_Applying_Capability_Maturity_Models_to_the_Evaluation_of_IT_Controls>.

[7] TechTimes. How The Internet Of Things Is The Perfect Target For DDoS Attacks And Data Breaches [interaktyvus]. 2017-01-14 [žiūrėta 2017 m. lapkričio 3 d.]. Prieiga per internetą: <http://www.techtimes.com/articles/191478/20170114/how-internet-of-things-devices-are-the-perfect-target-for-ddos-attacks-and-data-breaches.htm>.

[8] Ethical Hacking and Countermeasures by EC-Council. Introduction to Ethical Hacking. Module 01. Exam 312-50. 19-20 psl. [Žiūrėta 2017 m. kovo 18 d.].

[7] ELP frakcija. Kibernetinio saugumo apžvalga [interaktyvus]. 2016 m., ISSN 1392-6721 [žiūrėta 2017 m. rugsėjo 6 d.]. Prieiga per internetą: <http://apzvalga.eu/images/kibernetinis_saugumas.pdf>.

[9] ISACA. A simple definition of cybersecurity [interaktyvus]. ISACA News [žiūrėta 2017-05-15]. Prieiga per internetą: <http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296>.

[10] From information security to cyber security, R. Solms, J. Niekerk [interkatyvus]. 11 April 2013 [žiūrėta 2017 m. gruodžio 15d.]. Prieiga per internetą: <http://www.profsandhu.com/cs6393_s16/solms-2013.pdf>.

[11] Kibernetinis saugumas. Kibernetinio saugumo apžvalga [interaktyvus]. 2016 m. [žiūrėta 2017 m. gruodžio 13 d.]. Prieiga per internetą: <http://apzvalga.eu/images/kibernetinis_saugumas.pdf>.

[12] Lietuvos Respublikos Seimas. Lietuvos Respublikos Kibernetinio saugumo įstatymas [interaktyvus]. 2014 gruodžio 11d. [žiūrėta 2017 m. gruodžio 5 d.]. Prieiga per internetą: <https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4>.

[13] Douwe Korff. NIST Cyber Security Definitions [interaktyvus]. 2009 [žiūrėta 2017 m. gruodžio 13 d.]. Prieiga per internetą: <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CPDP%202015%20-%20KORFF%20Handout%20-%20DK150119.pdf>.

[14] NIST. An introduction to components of Framework [interaktyvus]. 2018 [žiūrėta 2017 m. gegužės 18 d.]. Prieiga per internetą: <https://www.nist.gov/cyberframework/new-framework>.

[15] Framework for Improving critical Infrastructure Cybersecurity. National Institute of Standards and Technology [interaktyvus]. April 16,2018 [žiūrėta 2018 m. balandžio 16 d.]. Prieiga per internetą: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

[16] Diffusion of innovations [interaktyvus]. Everett M. Rogers, 1983 [žiūrėta 2017 m. gegužės 17d.]. Prieiga per internetą: <https://teddykw2.files.wordpress.com/2012/07/everett-m-rogers-diffusion-of-innovations.pdf>.

[17] A. Mas, A. Mesquida, R.V. O'Connor, T. Rout, A. Dorling. Communications in Computer and Information Science, Software Process Improvement and Capability Determination. Ag 2017, Springer, psl. 430-438.

[18] M. Dowson (1998). Iteration in the Software Process, Proc 9th Int. Conf. on Software Engineering.

[19] Colette Rolland and Pernici, C. Thanos (1998). A Comprehensive View of Process Engineering. Proceedings of the 10th International Conference CAiSE'98. B. Lecture Notes in Computer Science 1413. Springer.

[20] C. A. Siegel, T. R. Sagalow, P. Serritella, Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security, Information security systems, Volume 11, 2002, Issue 4, psl. 33-49.

[21] Maturity based approach for ISMS Governance. K. Haufe. [interaktyvus]. [žiūrėta 2018 m. sausio 13 d.]. Prieiga per internetą: <https://e-archivo.uc3m.es/bitstream/handle/10016/25128/tesis_knut_haufe_2017.pdf?sequence=3>.

[22] Reference Architecture. CSA – Cloud Security Alliance. [interaktyvus]. 02/25/2013 [žiūrėta 2017 m. gruodžio 14 d.]. Prieiga per internetą: <https://downloads.cloudsecurityalliance.org/initiatives/tci/TCI_Reference_Architecture_v2.0.pdf>.

[23] A Guide to Cyber Risk: Managing the Impact of the Increasing Interconnectivity. Allianz Global Corporate & Specialty [interaktyvus]. September 2015 [žiūrėta 2017 m. gruodžio 5 d.]. Prieiga per internetą: <http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf>.

[24] Security Engineering Best Practices. K. Ferraiolo. [interaktyvus]. [žiūrėta 2018 m. sausio 13 d.]. Prieiga per internetą: <https://csrc.nist.gov/csrc/media/publications/conference-paper/1999/10/21/proceedings-of-the-22nd-nissc-1999/documents/papers/t02.pdf>.

[25] Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. R. ROSS, M. McEVILLEY, J. C. OREN [interaktyvus]. November 2016 [žiūrėta 2017 m. lapkričio 14 d.]. Prieiga per internetą: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf>.

[26] Antrinė kiekybinių duomenų analizė [interaktyvus]. Dr. Eglė Butkevičienė ir dokt. Aida Vaicekauskaitė, 2010 [žiūrėta 2017 m. rugsėjo 9 d.]. Prieiga per ineternetą: <http://www.lidata.eu/files/mokymai/kiek2/Antrine_kiekybiniu_duomenu_analize_20111111.pdf>.

[27] Boronowsky, M., Woronowicz, T., Mitasiunas, A. Bonita – Improve Transfer from Universities for Regional Development.. [interaktyvus]. The Proceedings of the 3rd ISPIM Innovation Symposium held in Quebec City, 2010 [žiūrėta 2017 m. lapkričio 16 d.]. Prieiga per internetą: <http://www.ispim.org/members/proceedings/Quebec10/commonfiles/files/26728727_Paper.pdf>.

[28] The New York Times. Computing Goes to the Cloud. So Does Crime [interaktyvus]. 2014-1202 [žiūrėta 2016 m. gegužės 14 d.]. Prieiga per internetą: <https://bits.blogs.nytimes.com/2014/12/02/computing-goes-to-the-cloud-so-does-crime/?_r=0>.

[29] Computers & Security. D. Gritzalis, G. Tejay. Volume 38 pp October 2013. Psl. 97-102.

[30] Information technology — Process assessment — An integrated process capability assessment model for Enterprise processes. ISO/IEC 33071:2016.

[31] Information technology -- Process assessment -- Process measurement framework for assessment of process capability. ISO/IEC 33020:2015.

[32] ISO/IEC 27000 family - Information security management systems. 2017 m.

PRIEDAI

Priedas Nr. 1. Informacijos saugumą užtikrinančių elementų paaiškinimas

(1) Konfidencialumas suprantamas kaip užtikrinimas, jog informacija yra pasiekiama tik tiems, kurie turi autorizuotą priėjimą prie jos. Konfidencialumo pažeidimai pasireiškia, pavyzdžiui, dėl netinkamo informacijos perdavimo valdymo ar įsilaužimo į sistemą. Konfidencialumo kontrolėms priklauso duomenų klasifikavimas, duomenų kodavimas, taipogi ir tinkamas duomenų naikinimas.

(2) Vientisumas aiškinamas kaip duomenų ar resursų patikimumas turint omenyje netinkamų ar neautorizuotų pakeitimų prevenciją. Tai užtikrinimas, jog informacija pasieks adresatą teisinga jos pakeitimo atžvilgiu. Priemonės palaikyti duomenų vientisumui gali būti sumos patikrinimas (skaičius gautas iš tarkime vienakryptės matematinės funkcijos tam, kad patikrinti, ar duotas duomenų blokas nėra pakeistas) ir prieigų valdymas (kas leidžia užtikrinti, jog tik tikslingai parinkti žmonės gali atnaujinti, pridėti ar ištrinti duomenis taip saugant jų vientisumą).

(3) Pasiekiamumas yra skirtas užtikrinti tai, jog sistemos atsakingos už informacijos pristatymą, laikymą, apdorojimą yra pasiekiamos, kai tai yra reikalinga autorizuotiems asmenims. Priemonės išlaikyti duomenų pasiekiamumą gali būti sistemų disko nereikalingo masyvo naikinimas, sugrupuotos mašinos, antivirusinė programinė įranga sustabdyti plintančius virusus nuo tinklo naikinimo, paskirstytos paslaugos atjungimo atakos prevencinės sistemos.

(4) Autentiškumas apibūdina komunikacijos, dokumentavimo ar kitų bet kokių duomenų, kurie užtikrina nesuklastojamumą, nesugadinimą charakteristikas. Pagrindine autentiškumas skirtas patvirtinti, jog vartotojas ir yra tas, kuriuo dedasi esąs. Taikomos kontrolės, tokios kaip biometrinės priemonės, išmanios kortelės ir elektroniniai parašai, užtikrina duomenų, pervedimų, komunikacijos, dokumentų autentiškumą.

(5) Galimybės nepripažinti nebuvimas yra būdas nustatyti, pavyzdžiui, jog siuntėjas, kuris išsiuntė pranešimą, negali vėliau to paneigti, taip pat kaip ir pranešimo gavėjas. Tam užtikrinti organizacijos ar individualūs asmenys naudoja elektroninius parašus.

Priedas Nr. 2. Palyginimui naudotas kibernetinio saugumo proceso etaloninis modelis sukurtas remiantis artimais gebėjimo modeliais

Kibernetinio saugumo proceso etaloninis modelis sukurtas remiantis ISO 33004 programų inžinerijos standarto reikalavimais. Modelis sudarytas iš trijų procesų kategorijų – inžinerinių procesų, pagalbinių procesų ir organizacinių procesų. Kiekvienas atskiras procesas aprašytas identifikatoriumi – trimis pirmosiomis kategorijos pavadinimo raidėmis ir skaitine reikšme, pavadinimu, paskirtimi ir rezultatais.

Organizacinių procesų kategorija

Organizacinių procesų kategorija įgalina kibernetinio saugumo inžinerinius procesus, užtikrina atitinkamus resursus, jų teisingą valdymą ir tinkamą kompetenciją, taip pat sąmoningumo ir žinių bazės ugdymą. Visa tai leis inžineriniams procesams veikti.

Strategijos ir politikų valdymas

ORG01	Strategijos ir politikų valdymas	
	Paskirtis	Rezultatai
	Įgalinti ir formalizuoti kibernetinio saugumo procesą organizacijoje.	1) Užtikrintas vadovybės palaikymas. 2) Politikos atspindi strategiją. 3) Rolės ir atsakomybės yra apibrėžtos. 4) Politikos yra palaikomos. 5) Politikos yra detalizuotos į standartus. 6) Politikų išimtys yra valdomos.

IT turto valdymas

ORG02	IT turto valdymas	
	Paskirtis	Rezultatai
	Inventorizuoti turtą saugumo priemonių poreikio išsiaiškinimui ir užtikrinimui.	1) Suinventorizuotas IT turtas. 2) Užtikrintas nuolatinis aktualaus turto sąrašo palaikymas. 3) Turtas suklasifikuotas ir detaliai aprašytas. 4) Turto gyvavimo ciklas yra dokumentuotas ir aktualus. 5) Pakeitimai yra patvirtinami formaliai. 6) Turto valdymui naudojami automatizuoti įrankiai.

Rizikos valdymo programa

ORG03	Rizikos valdymo programa	
	Paskirtis	Rezultatai
	Prioretizuoti ir tinkamai valdyti organizacijos resursus ginantis nuo išorės grėsmių valdant	1) Rizikos yra vertinamos reguliariu būdu.

	pažeidžiamumus ir atsižvelgiant į kylančias grėsmes.	2) Rizikos valdymo programa apima kibernetinių rizikų identifikavimą, vertinimą, riziką mažinančių priemonių įgyvendinimą, stebėjimą. 3) Vadovybė stebi rizikų valdymo procesą, riziką mažinančių priemonių įgyvendinimą. 4) Kibernetinio saugumo funkcija turi aiškią tiesioginę atskaitomybės liniją, kuri nesukelia interesų konflikto.

Resursų užtikrinimas

ORG04	Resursų užtikrinimas	
	Paskirtis	Rezultatai
	Prioretizuoti ir tinkamai valdyti organizacijos resursus ginantis nuo išorės grėsmių valdant pažeidžiamumus ir atsižvelgiant į kylančias grėsmes.	1) Kibernetinio saugumo funkcija turi dedikuotus resursus. 2) Taikomas formalus procesas kibernetinio saugumo įrankių ir resursų poreikiui vertinti. 3) Kibernetinio saugumo komanda turi reikiamas žinias ir įgūdžius reikiamus pozicijai. 4) Darbuotojams atliekama asmens patikra.

Mokymų programos valdymas

ORG05	Mokymų programos	
	Paskirtis	Rezultatai
	Mažinti žmogiškųjų klaidų, galinčių įtakoti kibernetinio saugumo riziką, tikimybę.	1) Kibernetinio saugumo mokymai yra atliekami reguliariai ne rečiau kaip kartą metuose. 2) Organizacija turi programą nuolatiniam kibernetinio saugumo kompetencijų didinimui. 3) Organizacija vertina mokymų efektyvumą. 4) Mokymai yra specializuoti pagal poreikį ir kylančias grėsmes. 5) Medžiaga yra lengvai prieinama visiems darbuotojams bet kada. 6) Vadovybė yra apmokoma atsižvelgiant į darbo atsakomybes.

Kultūros puoselėjimas

ORG06	Kultūros puoselėjimas	
	Paskirtis	Rezultatai
	Kibernetinio saugumo užtikrinimas priklauso nuo organizacijos požiūrio ir saugumo kultūros suvokimo.	1) Vadovybė prisiima atsakomybę dėl kibernetinio saugumo. 2) Vadovybė skleidžia kibernetinio saugumo supratimą organizacijos viduje. 3) Organizacijos darbuotojai formaliai yra supažindinti su galiojančiais reikalavimais. 4) Kibernetinio saugumo rizikos yra aptariamos vadovybės susitikimuose. 5) Darbuotojai turi aiškų suvokimą apie kibernetinį saugumą, incidentų eskalavimą.

		6) Organizacija dalinasi geriausiomis kibernetinio saugumo praktikomis atitinkamame sektoriuje.

Inžinerinių procesų kategorija

Kategorija sudaryta iš pirminių procesų reikalingų kibernetinio saugumo proceso įgalinimui ir vykdymui organizacijoje.

Reikalavimų valdymas

INZ01	Reikalavimų valdymas	
	Paskirtis	Rezultatai
	Aiškūs ir suprantami reikalavimai įvairiuose dokumentacijos lygiuose.	1) Reikalavimai yra dokumentuojami. 2) Formaliai užtikrintas aukšto lygio reikalavimų detalizavimas. 3) Reikalavimai įgyvendinami remiantis rizikų vertinimu. 4) Reikalavimai patvirtinami suinteresuotų padalinių. 5) Reikalavimų kūrimo procese atsižvelgiama į technologiją.

Perimetro apsauga

INZ02	Perimetro apsauga	
	Paskirtis	Rezultatai
	Tinklo suskirstymas ir technologinėmis priemonėmis vykdoma perimetro apsauga bei kontrolė.	1) Organizacijos tinklo perimetras yra apibrėžtas. 2) Perimetras yra izoliuotas atitinkamomis saugumo priemonėmis. 3) Perimetras yra pilnai kontroliuojamas. 4) Perimetro stebėjimas yra įgyvendinamas remiantis anomalijų aptikimu. 5) Įgyvendintas juodųjų sąrašų principas, kuris palaikomas aktualus. 6) Bevieliam tinklui pritaikytos saugumo priemonės. 7) Turinys yra filtruojamas.

Konfigūracijos valdymas

INZ03	Konfigūracijos valdymas	
	Paskirtis	Rezultatai
	Sukonfigūruoti ir valdyti konfigūracijas taip, kad jos atitiktų kibernetinio saugumo politiką.	1) Konfigūravimas yra integruota keitimų proceso dalis. 2) Pakeitimai yra testuojami. 3) Pakeitimai konfigūracijose yra tvirtinami. 4) Pakeitimai nesudaro išimčių kibernetinio saugumo politikoje.

Privilegijų naudojimo valdymas

INZ04	Privilegijų naudojimo valdymas	
	Paskirtis	Rezultatai
	Kontroliuoti aukštos rizikos sistemas, vartotojus ir procesus tam skiriant atitinkamą sugriežtintą dėmesį.	1) Privilegijuoti vartotojai, sistemos ir procesai yra identifikuoti. 2) Vykdomas tapatybės valdymas. 3) Įgyvendintos autorizavimo paslaugos. 4) Įgyvendintos autentifikavimo paslaugos. 5) Privilegijų naudojimas yra stebimas. 6) Privilegijų naudojimas yra kontroliuojamas. 7) Privilegijų naudojimas yra ribojamas pagal poreikį.

Tinklo apsauga

INZ05	Tinklo apsauga	
	Paskirtis	Rezultatai
	Užtikrinti serveriuose esančios informacijos ir susijungimo priemonių saugumą.	1) Serverių infrastruktūra yra aiškiai dokumentuota. 2) Sprendimo architektūriniai principai atitinka saugumo politiką. 3) Konfidencialūs duomenys yra apsaugoti. 4) Įdiegtos prevencinės priemonės draudžiančios neleistinam programiniam kodui veikti.

Aplikacijų saugumas

INZ06	Aplikacijų saugumas	
	Paskirtis	Rezultatai
	Užtikrinti aplikacijų ir susijusių duomenų kanalų saugumą.	1) Naudojamų aplikacijų sąrašas yra palaikomas. 2) Įgyvendintas realaus laiko filtravimas. 3) Veikiančios aplikacijos lygio ugniasienės. 4) Pranešimai perduodami saugiu būdu.

Galutinių įrenginių apsauga

INZ07	Galutinių įrenginių apsauga	
	Paskirtis	Rezultatai
	Užtikrinti vartotojų naudojamų arba sisteminių įrenginių saugumą nuo kibernetinių atakų.	1) Patikima įranga yra atpažįstama techniniame lygyje. 2) Įranga gali būti atjungta nuo organizacijos tinklo. 3) Kenkėjiškas programinės kodas aptinkamas veikimo atpažinimo principu. 4) Inventorius yra kontroliuojamas. 5) Turinys yra filtruojamas.

Kriptografijos paslaugos

INZ07	Kriptografijos paslaugos	
	Paskirtis	Rezultatai
	Apsaugoti duomenis įvairiuose lygmenyse.	1) Duomenys yra kriptuojami naudojimo metu. 2) Duomenys yra kriptuojami perkėlimo metu. 3) Duomenys yra kriptuojami saugojimo metu.

		4) Naudojamos pasirašymo paslaugos. 5) Naudojami įvairūs kriptografijos metodai.

Saugumo būsenos stebėjimas ir kontrolė

INZ09	Saugumo būsenos stebėjimas ir kontrolė	
	Paskirtis	Rezultatai
	Stebėti ir aptikti, laiku pašalinti židinius keliančius grėsmę kibernetiniam saugumui.	1) Saugumo būsena yra matuojama. 2) Įdiegta programinė įranga leidžianti stebėti įvykius. 3) Įdiegta programinė įranga analizuojanti įvykius. 4) Programinė įranga aptinka anomalijas. 5) Anomalijos yra registruojamos. 6) Anomalijos yra valdomos.

Pasirengimas kibernetiniams įsilaužimams

INZ10	Pasirengimas kibernetiniams įsilaužimams	
	Paskirtis	Rezultatai
	Sumažinti nuostolius įvykus kibernetiniam incidentui.	1) Aprašytas kibernetinio incidento suvaldymo veiksmų planas. 2) Sukurtas incidentų registras. 3) Incidentai yra stebimi. 4) Prevencinės priemonės sumažinti incidentų tikimybę yra diegiamos po įvykusių incidentų. 5) Prevencinės priemonės sumažinti incidentų poveikį yra diegiamos po įvykusių incidentų.

Pakeitimų kontrolė

INZ11	Pakeitimų kontrolė	
	Paskirtis	Rezultatai
	Kontroliuoti pakeitimus įgalinant konfigūracijų valdymą.	1) Auditas yra nepriklausoma funkcija. 2) Auti rekomendacijos yra dokumentuojamos. 3) Audito rekomendacijos yra įgyvendinamos. 4) Auditas seka rekomendacijų įgyvendinimą.

Atnaujinimų, kodų pataisymų valdymas

INZ12	Atnaujinimų, kodų pataisymų valdymas	
	Paskirtis	Rezultatai
	Užtikrinti, kad įranga būtų laiku atnaujinta ir taip išvengti žinomų pažeidžiamumų išnaudojimo.	1) Atnaujinimai yra diegiami automatizuotai. 2) Atnaujinimai yra diegiama centralizuotai. 3) Atnaujinimai yra gaunami centralizuotai. 4) Atnaujinimai įdiegiami suplanuotai. 5) Atnaujinimai testuojami prieš juos diegiant. 6) Naudojama tik naujausia programinė įranga.

Pagalbinių procesų kategorija

Pagalbinių procesų kategorija skiriama tam, kad kibernetinio saugumo funkcijos įgalinimas būtų pakankamas ir užtikrintas. Dauguma procesų tiesiogiai susiję su siekimu mažinti likutinių klaidų skaičių.

Atitikties testavimas

PAG01	Atitikties testavimas	
	Paskirtis	Rezultatai
	Užtikrinti, jog kibernetinio saugumo kontrolės priemonės yra atitinkamos ir tenkina reikalavimus.	1) Testavimas yra atliekamas apimant visas kibernetinio saugumo sritis. 2) Testavimas yra nuolatinis procesas. 3) Testavimo rezultatai yra dokumentuojami. 4) Testavimo pastebėjimai yra ištaisomi.

Auditavimas ir neatitikimų stebėjimas

PAG02	Auditavimas ir neatitikimų stebėjimas	
	Paskirtis	Rezultatai
	Įgalinti kelių lygių priežiūros kontrolę siekiant sumažinti klaidų skaičių.	1) Auditas yra nepriklausoma funkcija. 2) Auti rekomendacijos yra dokumentuojamos. 3) Audito rekomendacijos yra įgyvendinamos. 4) Auditas seka rekomendacijų įgyvendinimą.

Paskyrų prieigų priežiūra

PAG05	Paskyrų prieigų priežiūra	
	Paskirtis	Rezultatai
	Užtikrinti, kad paskyros ir prieigos nėra kompromituotos.	1) Paskyros yra audituojamos pagal apibrėžtas procedūras. 2) Prieigos yra audituojamos pagal apibrėžtas procedūras. 3) Prieigos yra suteikiamos tik pagal poreikį. 4) Paskyros yra tvarkomos visą gyvavimo ciklą.

Įsilaužimų imitavimas

PAG06	Įsilaužimų imitavimas	
	Paskirtis	Rezultatai
	Sumažinti klaidų palikimo tikimybę.	1) Įsiskverbimų testavimai atliekami nepriklausomos funkcijos. 2) Įsiskverbimų testavimai dokumentuojami. 3) Įsiskverbimų testavimai atliekami reguliariai. 4) Įsiskverbimų testavimų metu aptiktos klaidos yra taisomos. 5) Klaidų taisymas yra stebimas.

Duomenų panaudojamumo valdymas

PAG06	Duomenų panaudojamumo valdymas	
	Paskirtis	Rezultatai
	Užtikrinti duomenų saugumą visais gyvavimo ciklo etapais.	1) Duomenys yra registruojami. 2) Duomenys yra valdomi. 3) Nereikalingi duomenys yra saugiai pašalinami. 4) Vykdoma duomenų praradimo prevencija. 5) Užtikrinamas duomenų pasiekiamumas.

Priedas Nr. 3. Kibernetinio saugumo proceso gebėjimo vertinimo modelio pritaikymas organizacijoje

INZ.IDN01	**IT turto valdymas**				
	Bazinės praktikos	#1 Respondento vertinimas	2# Respondento vertinimas	Vertinimo vidurkis	Vertinimo kategorija
	BP.1: Inventorizuoti fizinius prietaisus organizacijoje. [Rezultatas: 1]	65 %	55 %	60 %	L
	BP.2: Inventorizuoti organizacijos sistemas. [Rezultatas: 2]	85 %	70 %	78 %	L
	BP.3: Inventorizuoti organizacijos turimą programinę įrangą. [Rezultatas: 3]	85 %	80 %	83 %	L
	BP.4: Dokumentuoti organizacijos duomenų srautus. [Rezultatas: 4]	50 %	45 %	48 %	P
	BP.5: Kataloguoti išorines informacijos sistemas. [Rezultatas: 5]	98 %	80 %	90 %	F
	BP.6: Prioretizuoti įvairius organizacijos resursus pagal jų sukuriamą vertę verslui. [Rezultatas: 6]	100 %	90 %	95 %	F
	BP.7: Naudoti automatizavimą turto valdymui. [Rezultatas: 7]	25 %	15 %	20 %	P
	BP.8: Apibrėžti kibernetinio saugumo roles ir atsakomybes organizacijoje. [Rezultatas: 8]	95 %	97 %	96 %	F
	Bendras vidurkis	***75 %***	***67 %***	***71 %***	***L***

INZ.ID	**Kibernetinio saugumo rizikos vertinimas**				
	Bazinės praktikos	#1 Respondento vertinimas	2# Respondento vertinimas	Vertinimo vidurkis	Vertinimo kategorija

	BP.1: Identifikuoti pažeidžiamumus turtui. [Rezultatas: 1]	45 %	32 %	39 %	P
	BP.2: Naudoti kibernetinio saugumo žvalgybos informaciją, gautą iš įvairių informacijos dalinimosi platformų, rizikos vertinime. [Rezultatas: 2]	12 %	5 %	9 %	N
	BP.3: Identifikuoti išorines ir vidines grėsmes rizikos vertinimui. [Rezultatas: 3]	56 %	70 %	63 %	L
	BP.4: Identifikuoti potencialų poveikį verslui. Jį išmatuoti. [Rezultatas: 4]	90 %	98 %	94 %	F
	BP.5: Naudotis patvirtinta rizikos valdymo metodologija. [Rezultatas: 5]	100 %	100 %	100 %	F
	BP.6: Prioretizuoti rizikos švelninimo priemones. [Rezultatas: 6]	100 %	100 %	100 %	F
	BP.7: Įtraukti vadovybę į rizikų vertinimą. [Rezultatas: 7]	40 %	60 %	50 %	P
	Bendras vidurkis	***63 %***	***66 %***	***65 %***	***L***

INZ.APS01	**Tapatybės ir prieigų valdymas**				
	Bazinės praktikos	#1 Respondento vertinimas	2# Respondento vertinimas	Vertinimo vidurkis	Vertinimo kategorija
	BP.1: Autorizuoti įrenginius, vartotojus ir procesus. [Rezultatas: 1]	80 %	70 %	75 %	L
	BP.2: Valdyti autorizuotų įrenginių, vartotojų, procesų kredencialus. [Rezultatas: 1]	90 %	85 %	88 %	F
	BP.3: Valdyti fizinę prieigą prie	90 %	70 %	80 %	L

	organizacijos turto. [Rezultatas: 2]				
	BP.4: Valdyti nuotolinę prieigą prie organizacijos turto. [Rezultatas: 3]	40 %	55 %	48 %	P
	BP.5: Valdyti prieigos teises organizacijoje. [Rezultatas: 4]	60 %	45 %	53 %	L
	BP.6: Apsaugoti tinklo vientisumą. [Rezultatas: 5]	80 %	72 %	76 %	L
	BP.7: Priskirti tapatybes kredencialams. [Rezultatas: 6]	95 %	80 %	88 %	F
	BP.8: Autentifikuoti vartotojus, įrenginius ir kitą turtą. [Rezultatas: 7]	65 %	78 %	72 %	L
	BP.9: Riboti privilegijų naudojimą pagal poreikį. [Rezultatas: 8]	55 %	70 %	63 %	L
	Bendras vidurkis	***73 %***	***69 %***	***71 %***	***L***

INZ.APS02	**Duomenų saugumas**				
	Bazinės praktikos	#1 Respondento vertinimas	2# Respondento vertinimas	Vertinimo vidurkis	Vertinimo kategorija
	BP.1: Apsaugoti laikomus duomenų talpyklose organizacijos duomenis. [Rezultatas: 1]	80 %	90 %	85 %	L
	BP.2: Apsaugoti perkeliamus duomenis. [Rezultatas: 2]	70 %	58 %	64 %	L
	BP.3: Valdyti turtą formaliai, dokumentuoti viso gyvavimo ciklo metu. [Rezultatas: 3]	85 %	80 %	83 %	L
	BP.4: Palaikyti adekvatų pajėgumų lygį, kuris leistų užtikrinti pasiekiamumą. [Rezultatas: 4]	70 %	90 %	80 %	L
	BP.5: Įgyvendinti apsaugą nuo duomenų	25 %	40 %	33 %	P

	nutekinimo. [Rezultatas: 5]				
	BP.6: Naudoti vientisumo patikrinimo mechanizmus. [Rezultatas: 6]	15 %	33 %	24 %	P
	BP.7: Atskirti plėtros ir bandymo aplinkas nuo produkcinės aplinkos. [Rezultatas: 7]	95 %	100 %	98 %	F
	BP.8: Naudoti vientisumo patikrinimo mechanizmus patikrinti techninės įrangos vientisumą. [Rezultatas: 8]	60 %	45 %	53 %	L
	Bendras vidurkis	***63 %***	***67 %***	***65 %***	***L***

INZ.APS03	**Priežiūra (palaikymas)**				
	Bazinės praktikos	#1 Respondento vertinimas	2# Respondento vertinimas	Vertinimo vidurkis	Vertinimo kategorija
	BP.1: Naudoti patvirtintus įrankius organizacijos turto priežiūrai. [Rezultatas: 1]	85 %	60 %	73 %	L
	BP.2: Dokumentuoti organizacijos turto priežiūrą. [Rezultatas: 2]	70 %	55 %	63 %	L
	BP.3: Patvirtinti priežiūrą nuotoliniu būdu. [Rezultatas: 3]	60 %	36 %	48 %	P
	BP.4: Dokumentuoti priežiūrą, atliekamą nuotoliniu būdu. [Rezultatas: 4]	72 %	80 %	76 %	L
	BP.5: Naudoti autorizuotas prieigas priežiūrai nuotoliniu būdu. [Rezultatas: 5]	85 %	95 %	90 %	F
	Bendras vidurkis	***74 %***	***65 %***	***70 %***	***L***

INZ.A	**Apsaugančios technologijos**				
	Bazinės praktikos	#1 Respondento vertinimas	2# Respondento vertinimas	Vertinimo vidurkis	Vertinimo kategorija

	BP.1: Rinkti audito įvykius iš sistemų. [Rezultatas: 1]	85 %	75 %	80 %	L
	BP.2: Peržiūrėti audito įvykių įrašus. [Rezultatas: 2]	10 %	25 %	18 %	P
	BP.3: Valdyti keičiamąsias laikmenas. [Rezultatas: 3]	50 %	60 %	55 %	L
	BP.4: Naudoti tik reikiamas funkcijas sistemose pagal konfigūraciją. [Rezultatas: 4]	80 %	56 %	68 %	L
	BP.5: Apsaugoti komunikacijos tinklus. [Rezultatas: 5]	80 %	95 %	88 %	F
	BP.6: Valdyti mechanizmus, kurie leidžia įgyvendinti atsparumo reikalavimus. [Rezultatas: 6]	85 %	100 %	93 %	F
	Bendras vidurkis	***65 %***	***69 %***	***67 %***	***L***

INZ.APT01	**Anomalijos ir įvykiai**				
	Bazinės praktikos	#1 Respondento vertinimas	2# Respondento vertinimas	Vertinimo vidurkis	Vertinimo kategorija
	BP.1: Valdyti bazinį tinklo operacijų saugumo lygį. [Rezultatas: 1]	60 %	69 %	65 %	L
	BP.2: Aptikti incidentus. [Rezultatas: 2]	75 %	60 %	68 %	L
	BP.3: Analizuoti aptiktus incidentus siekiant suprasti atakos principus. [Rezultatas: 2]	80 %	30 %	55 %	L
	BP.4: Koreliuoti įvykių duomenis iš įvairių sistemų. [Rezultatas: 3]	55 %	50 %	53 %	L
	BP.5: Apskaičiuoti įvykių poveikį. [Rezultatas: 4]	40 %	35 %	38 %	P
	BP.6: Nustatyti incidentų aliarmo ribas	85 %	90 %	88 %	F

	siekiant išvengti per didelio netikro pavojaus signalų. [Rezultatas: 5]				
	Bendras vidurkis	***66 %***	***56 %***	***61 %***	***L***

INZ.APT02	**Nuolatinis saugumo stebėjimas**				
	Bazinės praktikos	#1 Respondento vertinimas	2# Respondento vertinimas	Vertinimo vidurkis	Vertinimo kategorija
	BP.1: Stebėti tinklą siekiant aptikti potencialius kibernetinio saugumo įvykius. [Rezultatas: 1]	65 %	50 %	58 %	L
	BP.2: Stebėti fizinę aplinką siekiant aptikti potencialius kibernetinio saugumo incidentus. [Rezultatas: 2]	80 %	85 %	83 %	L
	BP.3: Stebėti personalo veiklą siekiant aptikti potencialius kibernetinio saugumo incidentus. [Rezultatas: 3]	65 %	50 %	58 %	L
	BP.4: Aptikti kenkėjišką kodą. [Rezultatas: 4]	80 %	55 %	68 %	L
	BP.5: Aptikti neautorizuotą mobilų kodą. [Rezultatas: 5]	60 %	75 %	68 %	L
	BP.6: Stebėti išorės tiekėjų paslaugų veiklą siekiant aptikti potencialius kibernetinio saugumo incidentus. [Rezultatas: 6]	40 %	70 %	55 %	L
	BP.7: Atlikti neautorizuoto personalo, prisijungimų, įrenginių, programinės įrangos stebėjimą. [Rezultatas: 7]	85 %	90 %	88 %	F
	BP.8: Atlikti pažeidžiamumų	100 %	100 %	100 %	F

	skanavimus. [Rezultatas: 8]				
	Bendras vidurkis	***72 %***	***72 %***	***72 %***	***L***

INZ.APT03	**Aptikimo procesas**				
	Bazinės praktikos	#1 Respondento vertinimas	2# Respondento vertinimas	Vertinimo vidurkis	Vertinimo kategorija
	BP.1: Tinkamai apibrėžti roles ir atsakomybes aptikimo procese. [Rezultatas: 1]	95 %	80 %	88 %	F
	BP.2: Suderinti aptikimo veiklas su kitais galiojančiais ir taikomais reikalavimais. [Rezultatas: 2]	80 %	95 %	88 %	F
	BP.3: Testuoti ir išbandyti aptikimo procesą. [Rezultatas: 3]	60 %	80 %	70 %	L
	BP.4: Komunikuoti įvykių aptikimo informaciją organizacijos viduje ir išorėje. [Rezultatas: 4]	90 %	85 %	88 %	F
	BP.5: Nuolatos tobulinti aptikimo procesus. [Rezultatas: 5]	50 %	60 %	55 %	L
	Bendras vidurkis	***75 %***	***80 %***	***78 %***	***L***

INZ.RGV01	**Reagavimo planavimas**				
	Bazinės praktikos	#1 Respondento vertinimas	2# Respondento vertinimas	Vertinimo vidurkis	Vertinimo kategorija
	BP.1: Aprašyti kibernetinio incidento suvaldymo planą. [Rezultatas: 1]	100 %	100 %	100 %	F
	BP.2: Vykdyti reagavimo planą kibernetinio incidento metu. [Rezultatas: 2]	100 %	100 %	100 %	F
	BP.3: Vykdyti reagavimo planą suvaldžius kibernetinį incidentą. [Rezultatas: 3]	95 %	80 %	88 %	F

	BP.4: Naudoti incidentų statistiką rizikų vertinimui. [Rezultatas: 4]	50 %	90 %	70 %	L
	Bendras vidurkis	***86 %***	***93 %***	***90 %***	***F***

INZ.RGV02	**Komunikacijos**				
	Bazinės praktikos	#1 Respondento vertinimas	2# Respondento vertinimas	Vertinimo vidurkis	Vertinimo kategorija
	BP.1: Personalui žinoti savo operacinius veiksmus vykstant ir įvykus kibernetiniam incidentui. [Rezultatas: 1]	70 %	80 %	75 %	L
	BP.2: Raportuoti kibernetinio saugumo incidentus pagal nustatytus kriterijus. [Rezultatas: 2]	55 %	68 %	62 %	L
	BP.3: Dalintis informacija apie kibernetinio saugumo įvykius pagal nustatytus planus. [Rezultatas: 3]	100 %	95 %	98 %	F
	BP.4: Koordinuoti kibernetinio saugumo incidentų informaciją tarp atsakingų asmenų ar institucijų pagal nustatytus planus. [Rezultatas: 4]	100 %	95 %	98 %	F
	BP.5: Dalintis informacija apie kibernetinio saugumo incidentus su išore siekiant platesnio kibernetinio saugumo sąmoningumo. [Rezultatas: 5]	50 %	30 %	40 %	P
	Bendras vidurkis	***75 %***	***74 %***	***75 %***	***L***

INZ.RGV03	**Analizė**				
	Bazinės praktikos	#1 Respondento vertinimas	2# Respondento vertinimas	Vertinimo vidurkis	Vertinimo kategorija

	BP.1: Tirti pranešimus iš aptikimo sistemų. [Rezultatas: 1]	75 %	55 %	65 %	L
	BP.2: Suprasti incidento poveikį ir tuo pasinaudoti atliekant tolimesnius veiksmus. [Rezultatas: 2]	80 %	67 %	74 %	L
	BP.3: Atlikti incidentų ekspertizę. [Rezultatas: 3]	80 %	60 %	70 %	L
	BP.4: Kategorizuoti incidentus pagal apibrėžtus planus ir kriterijus. [Rezultatas: 4]	30 %	60 %	45 %	P
	BP.5: Tikrinti pažeidžiamumus sužinomus iš išorės atitinkamų šaltinių. [Rezultatas: 5]	50 %	35 %	43 %	P
	Bendras vidurkis	***63 %***	***55 %***	***59 %***	***L***

INZ.RGV04	**Sušvelninimas**				
	Bazinės praktikos	#1 Respondento vertinimas	2# Respondento vertinimas	Vertinimo vidurkis	Vertinimo kategorija
	BP.1: Rinkti detalią informaciją apie incidentus ir ją panaudoti analizei. [Rezultatas: 1]	85 %	90 %	88 %	F
	BP.2: Valdyti incidentus. [Rezultatas: 2]	80 %	90 %	85 %	L
	BP.3: Valdyti naujai identifikuotus pažeidžiamumus rizikų valdymo pagrindu. [Rezultatas: 3]	60 %	45 %	53 %	L
	Bendras vidurkis	***75 %***	***75 %***	***75 %***	***L***

INZ.RGV05	**Tobulinimas**				
	Bazinės praktikos	#1 Respondento vertinimas	2# Respondento vertinimas	Vertinimo vidurkis	Vertinimo kategorija
	BP.1: Mokytis iš incidentų ir pagal tai atnaujinti procesus,	65 %	90 %	78 %	L

	sistemas ar planus. [Rezultatas: 1]				
	BP.2: Atnaujinti incidentų valdymo strategiją pagal vykstančius incidentus ir reikiamas priemones ar resursus tiems incidentams suvaldyti. [Rezultatas: 2]	30 %	45 %	38 %	P
	Bendras vidurkis	***48 %***	***68 %***	***58 %***	***L***

INZ.ATS01	**Atsistatymo planavimas**				
	Bazinės praktikos	#1 Respondento vertinimas	2# Respondento vertinimas	Vertinimo vidurkis	Vertinimo kategorija
	BP.1: Naudoti atsistatymo planą kibernetinio saugumo incidento metu. [Rezultatas: 1]	80 %	95 %	88 %	F
	BP.2: Naudoti atsistatymo planą kibernetinei atakai pasibaigus. [Rezultatas: 2]	90 %	100 %	95 %	F
	Bendras vidurkis	***85 %***	***98 %***	***92 %***	***F***

Priedas Nr. 4. Pilnai vykdomų procesų vertinimas antru lygiu

PA 2.1. Proceso valdymo vertinimas				
	INZ.RGV01 Reagavimo planavimas		INZ.ATS01 Atsistatymo planavimas	
	Respondentas #1	Respondentas #2	Respondentas #1	Respondentas #2
BP 2.1.1. Identifikuoti tikslus proceso atlikimui.	60 %	50 %	80 %	60 %
BP 2.1.2. Planuoti ir stebėti proceso atlikimą užtikrinti identifikuotus tikslus.	55 %	40 %	60 %	40 %
BP 2.1.3. Pritaikyti proceso atlikimą.	30 %	15 %	45 %	20 %
BP 2.1.4. Apibrėžti atsakomybes ir įgaliojimus proceso atlikimui.	85 %	70 %	80 %	70 %
BP 2.1.5. Identifikuoti ir atlaisvinti resursus procesą atlikti pagal planą.	60 %	80 %	80 %	75 %
BP 2.1.6. Valdyti sąsajas tarp įsitraukusių šalių.	35 %	55 %	10 %	40 %
Bendras vidurkis	**54 %**	**52 %**	**59 %**	**51 %**

Apibendrinant procesas INZ.RGV01 reagavimo planavimas vertinant jį antru lygiu ir atsižvelgiant į abiejų respondentų atsakymų vidurkį yra įvertintas 53 procentais ir pagal vertinimo skalę tai reiškia, jog proceso valdymas yra vykdomas (L).

Procesas INZ.ATS01 atsistatymo planavimas vertinant jį antru lygiu ir atsižvelgiant į abiejų respondentų atsakymų vidurkį yra atliekamas 55 procentais ir pagal vertinimo skalę tai reiškia, jog proceso valdymas yra vykdomas (L).

PA 2.2. Proceso darbo produktų valdymo vertinimas		
	INZ.RGV01	INZ.ATS01

	INZ.RGV01 Reagavimo planavimas		INZ.ATS01 Atsistatymo planavimas	
	Respondentas #1	Respondentas #2	Respondentas #1	Respondentas #2
BP 2.2.1. Apibrėžti reikalavimus darbo produktams.	50 %	30 %	90 %	100 %
BP 2.2.2. Apibrėžti reikalavimus darbo produktų dokumentavimui ir kontrolei.	10 %	15 %	25 %	20 %
BP 2.2.3. Identifikuoti, dokumentuoti ir kontroliuoti darbo produktus.	15 %	15 %	20 %	15 %
BP 2.1.4. Peržiūrėti ir pritaikyti darbo produktus taip, kad jie atitiktų iškeltus reikalavimus.	30 %	20 %	15 %	10 %
Bendras vidurkis	**26 %**	**20 %**	**38 %**	**36 %**

Apibendrinant proceso produktų darbo vertinimas tiek reagavimo planavimo procese, tiek atsistatymo planavimo procese yra dalinai vykdomas (P) atitinkamai respondentams vidutiniškai įvertinus 23 proc. ir 37 proc.