Finansuoja Europos Sąjunga

NAUJOS KARTOS LIETUVA

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Nacionalinis kibernetinio saugumo centras

Kibernetinio saugumo rizikos vertinimo metodika

2025 m.

Turinys

1. Įvadas

Atsižvelgdamas į vis didėjantį poreikį užtikrinti nuoseklų ir aukštos kokybės kibernetinio saugumo rizikos valdymą, Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (NKSC), vykdydamas jam pavestas funkcijas ir siekdamas stiprinti nacionalinį kibernetinį atsparumą, inicijavo šios metodikos rengimą.

Ši kibernetinio saugumo rizikos vertinimo metodika parengta remiantis standartais ISO/IEC 27005:2022, „BSI Standard 200-3“, „NIST SP 800-30 Revision 1“, „ENISA Risk Management Guidelines“, metodikomis ir rinkos tyrimais, įskaitant Europos Sąjungos šalių (Belgijos, Vokietijos, Slovakijos) tyrimus, Jungtinės Karalystės ir Singapūro partnerių kibernetinio saugumo vertinimo tyrimą, taip pat Lietuvoje atliktą būsimų Lietuvos Respublikos kibernetinio saugumo subjektų kibernetinio saugumo rizikos valdymo ir kibernetinio saugumo brandos lygio tyrimą.

Ši metodika parengta atsižvelgiant į nacionalinius ir tarptautinius teisės aktus, reglamentuojančius kibernetiniam saugumui kylančios rizikos (toliau – rizikos) valdymą, įskaitant:

- 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyvą (ES) 2022/2555 dėl aukšto bendro kibernetinio saugumo lygio visoje Sąjungoje (NIS2 direktyva) [1];
- Kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymą (2024 m. liepos 11 d. Nr. XIV-2902) [2];
- Kibernetinio saugumo reikalavimų aprašą, patvirtintą Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ pakeitimo“ [3];
- kitus galiojančius poįstatyminius teisės aktus, susijusius su rizikos valdymu viešajame ir privačiame sektoriuose.

Šioje metodikoje aprašomas rizikos valdymo procesas, pritaikytas mažo ir vidutinio dydžio organizacijoms, nepriklausomai nuo jų tipo ar sektoriaus.

Organizacija turi aiškiai nustatyti ir patvirtinti taikomą rizikos vertinimo metodiką. Organizacija gali pritaikyti šią metodiką pagal savo poreikius, tačiau visi pakeitimai turi būti dokumentuoti, pagrįsti ir patvirtinti vadovybės. Pasirinkta metodika turi užtikrinti efektyvų rizikos valdymo procesą, atitinkantį organizacijos specifiką ir teisinius reikalavimus.

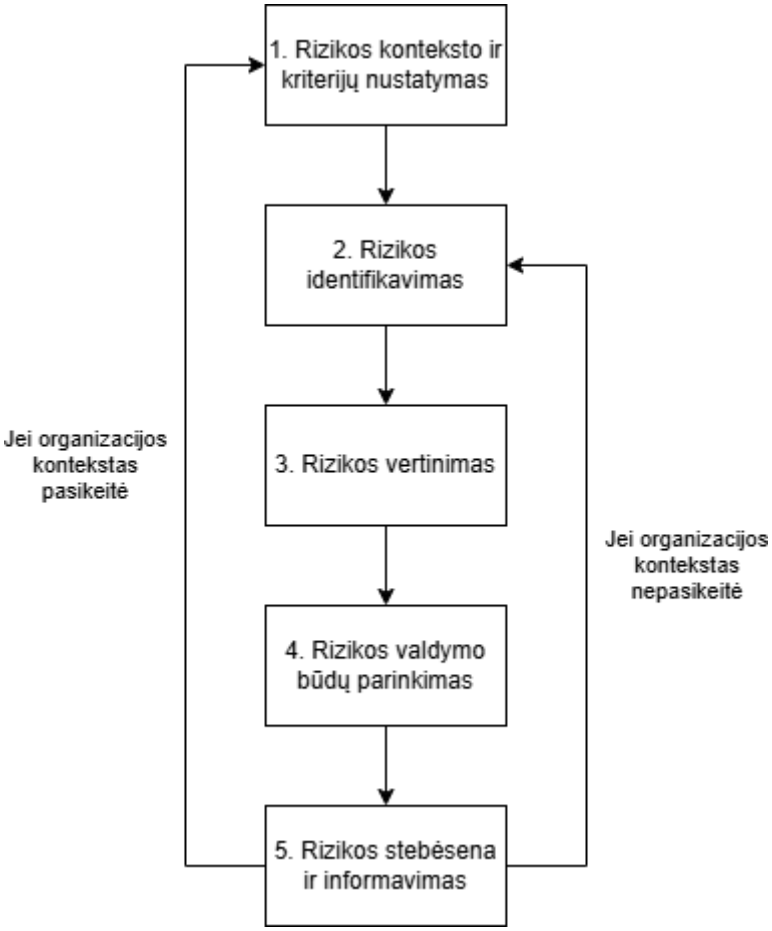
1.1 Rizikos vertinimo pavyzdys

Šioje metodikoje pateikiamas teorinis medicinos klinikų tinklui UAB „LitBaltMed“ kylančios rizikos vertinimo pavyzdys. Pateiktas pavyzdys padeda suprasti, kaip nustatomi kriterijai, grėsmės, pažeidžiamumai, identifikuojamas turtas, identifikuojama ir vertinama rizika, kaip pasirenkami rizikos valdymo būdai ir priemonės ir vykdomas rizikos stebėsenos organizavimas.

UAB „LitBaltMed“ – tai vidutinio dydžio medicinos klinikų tinklas, kurio pagrindinė būstinė įsikūrusi Vilniuje, o papildomos klinikos veikia Kaune, Klaipėdoje ir Panevėžyje. Įmonėje dirba apie 40 darbuotojų, o metinės pajamos siekia maždaug 10 mln. Eur. Įmonė teikia pirminės sveikatos priežiūros paslaugas, atlieka specializuotus tyrimus (rentgeno, laboratorinius) ir naudoja centralizuotą elektroninę pacientų duomenų sistemą, sujungiančią visas klinikas. Dėl jautrių pacientų duomenų tvarkymo ir strateginės svarbos sveikatos apsaugos srityje organizacija laikoma svarbiu subjektu pagal Kibernetinio saugumo subjektų registrą.

2. Rizikos konteksto ir kriterijų nustatymas

2.1 Rizikos valdymo proceso etapai



1. **Rizikos konteksto ir kriterijų nustatymas**
   - Nustatomi rizikos atlaikymo pajėgumo, apetito ir tolerancijos kriterijai

   Rizikos identifikavimas
   - Sudaromas turto registras.
   - Sudaromas rizikos registras, analizuojant grėsmes, pažeidžiamumus ir juos pritaikant turto vienetui ar grupei ir aprašant riziką.
3. Rizikos analizė ir vertinimas
   - Identifikuojamas prigimtinės rizikos lygis;
   - Įvertinami jau pritaikyti rizikos valdymo būdai ir priemonės.
   - Nustatomas dabartinis rizikos lygis.
4. Rizikos valdymo būdų ir priemonių parinkimas
   - Parenkamas rizikos valdymo būdas (priėmimas, mažinimas, perdavimas, vengimas).
   - Esant poreikiui numatomos rizikos valdymo priemonės.
   - Nustatomas galutinės (ateities būsena) rizikos lygis.
5. Rizikos stebėjimas ir informavimas
   - Atliekamas nuolatinis vidinių organizacijos pokyčių stebėjimas ir grėsmių žvalgyba.
   - Stebimas parinktų rizikos valdymo būdų pritaikymas ir priemonių įdiegimas.
   - Atliekama rizikos valdymo proceso peržiūra.

- Nustatomi stebėsenos rodikliai ir rizikos indikatoriai.

2.2 Organizacinio konteksto nustatymas

2.2.1 Suderinamumas su organizacijos masto rizikos valdymo modeliu

Rizikos vertinimo metodika turi būti suderinta su organizacijos masto rizikos valdymo metodika, siekiant, kad rizikos būtų išreikštos vienodu formatu. Jeigu organizacijos masto rizikos valdymo sistemos aspektai skiriasi nuo šioje metodikoje apibrėžtų, turėtų būti sukurtas ir aprašytas aiškus mechanizmas, kaip rizikos valdymas yra suderintas su organizacijos rizikos valdymu ir į jį integruotas.

Pavyzdys. UAB „LitBaltMed“ rizikos vertinimo suderinamumas su organizacijos masto rizikos vertinimo modeliu.

UAB „LitBaltMed“ rizikos vertinimo dokumentuose analizuojama, kokią riziką sukeltų darbuotojų trūkumas, sveikatos politikos pokyčiai ar finansavimo sumažėjimas, vertinamos grėsmės pacientų duomenų sistemai, galimos *ransomware* atakos ar tiekėjų informacinių technologijų (toliau – IT) sistemų pažeidžiamumai. Abi metodikos integruotos taikant vienodą rizikos vertinimo matricą, su tais pačiais poveikio ir tikimybės balais. Tai leidžia rizikas įtraukti į bendrą organizacijos rizikų žemėlapį ir prioretizuoti jas kartu su kitomis verslo rizikomis.

2.2.2 Rizikos vertinimo dokumentacija

Šiame skyriuje aptariami rizikos valdymo dokumentai, kuriuos organizacijos turi parengti, patvirtinti ir naudoti rizikos valdymo organizavimo procese.

Dokumentas	**Aprašymas**	**Atsakingas už parengimą**	**Atsakingas už patvirtinimą**
Rizikos valdymo tvarkos aprašas	Dokumentas, nustatantis rizikos valdymo principus, kriterijus, atsakomybę ir rizikos nustatymo, vertinimo ir valdymo procedūras. Dokumentas apibrėžia rizikos valdymo tikslus, taikymo sritį, atlaikymo pajėgumą, apetito ir tolerancijos kriterijus, sprendimų priėmimo kriterijus, rizikos valdymo procesų integravimo į organizacijos veiklą procesą.	Kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis, bendradarbiaujant su padalinių vadovais, išorės konsultantu (esant poreikiui).	Vadovybė
Turto katalogas	Dokumente inventorizuojami ir klasifikuojami organizacijos informaciniai ištekliai. Turto katalogu remiamasi atliekant rizikos vertinimą, tačiau šis dokumentas nėra visos organizacijos IT inventorizacijos sąrašas.	Kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis, bendradarbiaujant su turto savininkais ir kibernetinio saugumo rizikos vertinimo ir valdymo ekspertu (esant poreikiui).	Neturi būti patvirtintas

Rizikos registras	Tai pagrindinė rizikos valdymo ir komunikavimo priemonė, kurioje nustatomos ir aprašomos rizikos, vertinamas jų lygis ir priskiriamas valdymo būdas ir priemonės. Registru turėtų būti remiamasi priimant sprendimus, vykdant stebėseną ir siekiant užtikrinti, kad rizikos laipsnis atitiktų organizacijos nustatytą apetito bei tolerancijos limitus. Taip pat į rizikos registrą įtraukiami grėsmių, pažeidžiamumų ir valdymo priemonių katalogai.	Kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis, bendradarbiaujant su turto savininkais, kibernetinio saugumo rizikos vertinimo ir valdymo ekspertu (esant poreikiui).	Neturi būti patvirtintas
Rizikos valdymo planas	Strateginis dokumentas, kuriame nurodomos rizikos ir jų valdymo būdai ir priemonės, įskaitant terminus, atsakomybę ir išteklių reikalavimus rizikos kontrolės būdams ar priemonėms įgyvendinti. Papildomai gali būti parengtas finansinių priemonių planas, dokumentas ar jo priedas, detalizuojantis, kokios numatomos rizikos valdymo veiksmų, būdų, priemonių ir priežiūros išlaidos.	Kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis, bendradarbiaujant su turto savininkais ir kibernetinio saugumo rizikos vertinimo ir valdymo ekspertu (esant poreikiui).	Vadovybė
Rizikos vertinimo ataskaita	Dokumente pateikiami rizikos analizės rezultatai.	Kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis ir kibernetinio saugumo rizikos vertinimo ir valdymo ekspertu (esant poreikiui).	Vadovybė

Pastaba. Kiekviena organizacija gali pasirinkti, kokios formos ir kokio pobūdžio dokumentuose aprašyti rizikos valdymo procesą. Dokumentai gali būti sujungiami arba išskaidomi pagal organizacijos dydį ir poreikį. Svarbu, kad dokumentai būtų rengiami vadovaujantis aiškumo, atsekamumo ir tarpusavio suderinamumo principais.

2.2.3 Atsakomybės ir vaidmenys

Rizikos vertinimo procese dalyvauja įvairūs darbuotojai, kurių atsakomybė ir vaidmuo priklauso nuo organizacijos dydžio, sektoriaus, turimos kompetencijos ir taikomų teisinių reikalavimų. Šiame skyriuje

atsakomybė ir vaidmenys aprašomos apibendrintai. Detalesni aprašymai pateikti sąvokų sąrašo 4 skyriuje ir atitinkamuose metodikos skyriuose.

Rekomenduojama rizikos valdymo procese taikyti aiškų atsakomybės ir vaidmenų atskyrimo principą.

Vienas iš dažniausiai taikomų principų – trijų gynybos linijų modelis (angl. *The Three Lines of Defense Model*, LoD), užtikrinantis atsakomybių ir vaidmenų atskyrimo (angl. *segregation of duties*) principą. LoD padeda užtikrinti, kad rizikos vertinimo, valdymo būdų ir priemonių įgyvendinimo ir nepriklausomo vertinimo funkcijos būtų vykdomos skirtingų padalinių ar asmenų.

Taip pat svarbu, kad aukštesnės gynybos linijos darbuotojai nebūtų pavaldūs žemesnės gynybos linijos darbuotojams, nes atitikties užtikrinimo ir tvirtinimo procesuose turi būti užtikrinamas nešališkumas. Tai padeda išvengti interesų konflikto, didina kontrolės efektyvumą ir užtikrina nešališką grėsmių ir rizikos valdymą. Pateiktoje lentelėje pateikiamas teorinis šių principų pagrindu sukurtas atsakomybių ir vaidmenų modelis, tačiau jis gali būti keičiamas priklausomai nuo sektoriaus, teisinio reguliavimo ir organizacijos brandos.

Pagrindinės atsakomybės ir vaidmenys

Gynybos linija	**Vaidmenys**	**Funkcijos ir atsakomybės**
1-oji linija – operacinė gynyba	Turto savininkas (-ai) (angl. *asset owner*) Ir / ar Rizikos savininkas (-ai) (angl. *risk owner*)	Atlieka savo įprastas darbo funkcijas, tačiau rizikos vertinimo metu įtraukiamas į procesą, jei reikalingos jo specifinės žinios. Turto / rizikos savininkas gerai išmano prižiūrimą sistemą ir gali konsultuoti turto / veiklos poveikio, sistemos priklausomumų, pažeidžiamumų, rizikos valdymo priemonių klausimais, taip pat dalyvauja rizikos rodiklių nustatymo procese.
2-oji linija – rizikos ir atitikties užtikrinimas	Kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis (angl. CISO / ISO) Ir / ar Kibernetinio saugumo rizikos vertinimo ir valdymo specialistas Ir / ar Organizacijos masto rizikos valdymo pareigūnas (angl. *risk manager*)	Kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis (angl. CISO / ISO) yra pagrindinis rizikos valdymo proceso koordinatorius organizacijoje. Jis atsakingas už viso proceso vykdymą – nuo planavimo iki stebėsenos – ir dalyvauja visuose rizikos vertinimo ir valdymo etapuose. Jis taip pat rengia rizikos valdymo dokumentus ir paskirsto kitus su procesu susijusius vaidmenis. Kibernetinio saugumo rizikos vertinimo ir valdymo specialistas yra kibernetinio saugumo vadovo ar saugos įgaliotinio paskirtas asmuo, teikiantis ekspertinę pagalbą viso proceso metu. Jis gali būti organizacijos vidaus ekspertas (pvz., LoD specialistas) arba išorės konsultantas. Specialistas aktyviai dalyvauja visuose rizikos vertinimo etapuose,

		padėdamas užtikrinti metodinį tikslumą ir duomenų pagrįstumą. Jeigu vykdomas organizacijosmasto (angl. *enterprise-level*) rizikos vertinimas, organizacijos masto rizikos valdymo pareigūnas (angl. *risk manager*) tampa viso organizacinio rizikos valdymo proceso savininku. Jis bendradarbiauja su kibernetinio saugumo vadovu ir (ar) saugos įgaliotiniu, siekdamas suderinti rizikos vertinimo metodikas, užtikrinti nuoseklų vertinimą visoje organizacijoje ir, jei turi reikiamą kompetenciją, prisideda prie kibernetinio saugumo rizikos vertinimo proceso.
3-ioji linija – nepriklausomas auditas	Vidaus / išorės auditoriai ir saugumo ekspertai	Vertina rizikos valdymo proceso atitiktį audito kriterijams, atlieka nepriklausomą rizikos valdymo proceso ir dokumentacijos vertinimą.

Valdymo organai, įskaitant vadovybę, patvirtina rizikos vertinimo ir valdymo tvarką ir kitas darbo efektyvumo užtikrinimo funkcijas, tačiau jie nėra priskiriami prie jokios gynybos linijos.

Pavyzdys. UAB „LitBaltMed“ atsakomybių ir vaidmenų pasiskirstymas.

Įrašyta į reguliuojamų subjektų sąrašą, UAB „LitBaltMed“ priėmė sprendimą paskirti kibernetinio saugumo vadovą, kuris atliks ir saugos įgaliotinio funkciją. Iki tol už kibernetinio saugumo klausimus buvo atsakingas tik IT administratorius. Saugos įgaliotinis, vadovaudamasis Kibernetinio saugumo įstatymu ir Kibernetinio saugumo reikalavimų aprašu, parengė rizikos vertinimo tvarką ir inicijavo rizikos valdymo procesą.

Kadangi saugos įgaliotinis, kaip antrosios gynybos linijos atstovas, neturėjo reikiamos kompetencijos savarankiškai atlikti rizikos vertinimą, jis pasitelkė išorės ekspertą kaip rizikos vertinimo ir valdymo ekspertą. Šis, vykdydamas rizikos vertinimo procesą, įtraukė ir pirmosios gynybos linijos atstovus – IT administratorių ir kitus atsakingus už tinklų ir informacinių sistemų (toliau – TIS) turtą savininkus. Turto savininkai pateikė informaciją apie sistemas, jų techninius sprendimus, infrastruktūrą, pažeidžiamumus ir trūkumus.

Siekdamas užtikrinti rizikos vertinimo suderinamumą su organizacijos bendrąja rizikos valdymo sistema, rizikos vertinimo ir valdymo ekspertas glaudžiai bendradarbiavo su organizacijos rizikos valdymo pareigūnu.

2.2.4 Rizikos vertinimo ciklai

Metodika taikoma reguliariems rizikos vertinimams, kurie turi būti atliekami ne rečiau kaip kartą per metus. Šioje metodikoje aprašomas vienas rizikos vertinimo ciklas, atspindintis organizacijos veiksmus per vienerių metų laikotarpį.

Rizikos vertinimo ciklą sudaro etapai, aprašyti metodikos 3 skyriuje.

Visi atlikti rizikos vertinimo dokumentai organizacijoje turėtų būti registruojami ir saugomi 3 metus nuo jų parengimo dienos, nes tai užtikrina rizikos valdymo proceso tęstinumą, skaidrumą ir atsekamumą. Tinkamai dokumentuoti rizikos vertinimo dokumentai leidžia per laiką stebėti rizikos lygio pokyčius, įvertinti įdiegtų rizikos valdymo būdų ir priemonių efektyvumą ir pagrįsti saugumo investicijų reikalingumą.

2.2.5 *Ad hoc* vertinimas

Metodika taip pat taikoma pagal poreikį atliekamiems *ad hoc* rizikos vertinimams, kai įvyksta incidentai, vadovybės sprendimu ir atsižvelgiant į organizacijos pokyčius ar grėsmių žvalgybos duomenis, pateiktus 3.4.1 ir 3.4.2 skyriuose.

Rizikos valdymo procese turi būti užtikrinta galimybė vykdyti *ad hoc* vertinimus, kai rizika kyla vykdant stebėseną ar tarp planuotų vertinimo ciklų. Kibernetinio saugumo vadovas arba jo įgaliotas asmuo, atsižvelgdamas į rizikos stebėsenos ir informavimo rezultatus (pvz., padidėjusių grėsmių signalus, incidentų pasikartojimų dažnumą, išorinių šaltinių informaciją apie pažeidžiamumą), inicijuoja rizikos vertinimo peržiūrą, kurios metu nustatoma, ar atsiradusi rizika yra nauja, ar reikšmingai pakitusi esama rizika. Iš naujo įvertinama rizikos tikimybė ir rizikos poveikio lygis, peržiūrimi taikomi rizikos valdymo būdai ir priemonės ir, jei būtina, atnaujinami turto, grėsmių ir pažeidžiamumų katalogai, rizikos registras ir rizikos valdymo planas.

Ad hoc vertinimas nėra išimtis, tai neatsiejama nuolatinės rizikos stebėsenos ir informavimo dalis, todėl turi būti vykdomas pagal bendruosius šios metodikos principus, užtikrinant dokumentavimą, vertinimo kriterijų nuoseklumą ir sprendimų atsekamumą.

Pavyzdys. UAB „LitBaltMed“ atliko *ad hoc* rizikos vertinimą.

UAB „LitBaltMed“, vykdydama nuolatinę rizikos stebėseną, nustatė, kad per paskutines tris savaites iš eilės pasikartojo incidentai, susiję su laikinu prieigos praradimu prie elektroninės medicininių duomenų ir receptų sistemos (EMDRS) visuose klinikų padaliniuose. Po šių kartotinių sutrikimų saugumo įgaliotinis inicijavo *ad hoc* rizikos vertinimą.

Nustatyta, kad dėl neseniai įdiegtos integracijos sistemos su nacionaline e. sveikatos duomenų baze padidėjo centralizuoto serverio apkrova. Ši integracijos sistema nebuvo tinkamai įvertinta planinio rizikos vertinimo etape, nes buvo įdiegta po paskutinio vertinimo. Rizikos vertinimo metu buvo peržiūrėta serverių infrastruktūra, įvertintas veiklos trikdžių poveikis visų klinikų pacientų aptarnavimui ir duomenų prieinamumui, taip pat pateiktos rekomendacijos dėl serverių talpos išplėtimo ir sistemos veikimo stebėsenos gerinimo. Vertinimo rezultatai įtraukti į turto katalogą, rizikos registrą ir valdymo planą, o sprendimą dėl papildomų priemonių finansavimo priėmė įmonės vadovybė.

Taip pat priimtas sprendimas atlikti rizikos vertinimą keičiant ar modernizuojant organizacijos TIS.

2.3 Rizikos kriterijų nustatymas

Kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis kartu su vadovybe įvertina ir nustato rizikos kriterijus, o prireikus suderina su organizacijos masto rizikos pareigūnu.

2.3.1 Rizikos atlaikymo pajėgumas

Rizikos atlaikymo pajėgumo kriterijus nustato didžiausią potencialią rizikos žalą, kurią organizacija gali prisiimti nesukeldama kritinių pasekmių veiklai. Šis strateginio lygio kriterijus nustato absoliučias ribas, kurių peržengimas keltų grėsmę organizacijos veiklos tęstinumui.

Įprastai šį kriterijų nustato organizacijos masto rizikos valdymo pareigūnas.

Rizikos atlaikymo pajėgumas turėtų būti išreikštas kiekybiškai, kai įmanoma, nustatant maksimalią finansinę ar operacinę žalą, kurią organizacija galėtų atlaikyti. Šis įvertinimas turėtų būti reguliariai peržiūrimas ir atnaujinamas atsižvelgiant į organizacijos išteklių, veiklos aplinkos ir strateginių tikslų pokyčius.

Rizikos atlaikymo pajėgumo kriterijus naudojamas poveikio vertinimo lentelėms sudaryti ir kalibruoti, siekiant užtikrinti, kad katastrofinis poveikio lygis (5) atspindėtų pasekmes organizacijai.

Organizacija turėtų nustatyti mažo (1) ir katastrofinio (5) poveikio lygių finansines ribas ir jas išreikšti procentais nuo metinių pajamų:

- 1 lygis (mažas poveikis) – rekomenduojama 0,2–1 % nuo metinių pajamų;
- 5 lygis (katastrofinis poveikis) – rekomenduojama 15–20 % nuo metinių pajamų.

Tarpinių lygių (2–4) ribos turėtų būti proporcingos šioms kraštutinėms reikšmėms. Metodikos 5.1 priede pateikta finansinio nuostolio skaičiuoklė automatiškai sugeneruos proporcingus tarpinius lygius.

Taip pat svarbu įvertinti ne tik finansinį poveikį, bet ir galimą žalą reputacijai, kiekvieno lygio poveikį veiklos tęstinumui, duomenų saugumui ar atitikčiai teisės aktams. Katastrofinis poveikis (5) turėtų atspindėti riziką, keliančią pavojų tolesniam organizacijos egzistavimui.

Šios procentinės išraiškos yra rekomenduojamos, bet ne privalomos. Organizacijos turėtų jas pritaikyti atsižvelgdamos į savo dydį, sektorių, finansinę padėtį ir kitus organizacijai specifiškus veiksnius.

Pavyzdys. UAB „LitBaltMed“ nustatė rizikos atlaikymo pajėgumo kriterijus.

UAB „LitBaltMed“, kurios metinės pajamos siekia 10 mln. Eur, nustatė rizikos atlaikymo pajėgumo kriterijus pagal finansinį ir veiklos tęstinumo aspektus.

Finansinis aspektas

Organizacijos strateginė analizė parodė, kad finansiniai nuostoliai, viršijantys 15 % metinių pajamų (1 500 000 Eur), sukeltų egzistencinę grėsmę veiklai, nes:

- būtų išnaudotos visos finansinės atsargos;
- tektų imti papildomą paskolą nepalankiomis sąlygomis;
- sumažėtų galimybės investuoti į technologijas;
- kiltų grėsmė neišlaikyti kvalifikuoto medicinos personalo.

UAB „LitBaltMed“ naudoja strateginius rizikos atlaikymo pajėgumo kriterijus nustačiusi savo rizikos poveikio lygio skalę pagal šią skaičiuoklę:

- 1 lygis (mažas poveikis) – mažiau nei 50 000 Eur (0–0,5 % nuo metinių pajamų);
- 2 lygis (reikšmingas poveikis) – 50 000–533 333 Eur (0,5–5,33 % nuo metinių pajamų);
- 3 lygis (rimtas poveikis) – 533 333–1 016 666 Eur (5,33–10,17 % nuo metinių pajamų);
- 4 lygis (kritinis poveikis) – 1 016 666–1 500 000 Eur (10,17–15 % nuo metinių pajamų);
- 5 lygis (katastrofinis poveikis) – daugiau nei 1 500 000 Eur (>15 % nuo metinių pajamų).

Veiklos tęstinumo aspektas

Organizacija strategiškai apibrėžė, kad katastrofinės pasekmės veiklai būtų, jei:

- daugiau nei 48 val. negali teikti pagrindinių sveikatos priežiūros paslaugų;
- praranda prieigą prie pacientų duomenų ilgiau nei 48 val.;
- netenka daugiau nei 25 % klientų.

Šis strateginis požiūris leidžia UAB „LitBaltMed“ aiškiai nustatyti, kokios rizikos kelia egzistencinę grėsmę ir reikalauja daug dėmesio ir išteklių, siekiant užtikrinti, kad organizacija nesusidurtų su neišvengiamai katastrofiškais padariniais.

UAB „LitBaltMed“ nustatė maksimalų toleruotiną neveikimo laiką kiekvienam rizikos poveikio lygiui:

- 1 lygis (mažas poveikis) – maksimalus toleruotinas neveikimo laikas iki 30 d.;
- 2 lygis (reikšmingas poveikis) – maksimalus toleruotinas neveikimo laikas iki 7 d.;
- 3 lygis (rimtas poveikis) – maksimalus toleruotinas neveikimo laikas iki 72 val.;
- 4 lygis (kritinis poveikis) – maksimalus toleruotinas neveikimo laikas iki 24 val.;
- 5 lygis (katastrofinis poveikis) – maksimalus toleruotinas neveikimo laikas iki 4 val.

2.3.2 Rizikos apetitas

Šioje metodikoje rizikos apetitas (angl. *risk apetite*) apibrėžiamas kaip priimtinumo lygis, kuris nurodo, kokio dydžio rizikas organizacija yra pasirengusi ir gali prisiimti. Rizikos apetitas nurodomas kaip rizikos lygis, didesnio lygio rizikoms turi būti pritaikyti rizikos valdymo būdai.

Rizikos lygio pavojingumas vertinamas nuo „labai mažas“ (1) iki „katastrofinis“ (5). Rizikos lygis nustatomas pagal rizikos poveikio ir tikimybės lygius, kurie nurodomi šios metodikos i 3.2.1.1 ir 3.2.1.2 skyriuose atitinkamai.

Organizacija, atsižvelgdama į savo veiklos pobūdį, strateginius tikslus ir išteklius, privalo nuspręsti, ar rizikos valdymo būdai bus taikomi žemai, vidutinei ar aukštai rizikai. Šis sprendimas turi būti pagrįstas organizacijos gebėjimu prisiimti riziką ir turėtų būti aiškiai dokumentuotas. Šios metodikos 5.3 priede pateiktas klausimynas padės priimti sprendimus ir atsirinkti, į kokius veiksnius atsižvelgti nustatant apetito lygį.

2.3.3 Rizikos tolerancija

Rizikos tolerancija (angl. *risk tolerance*) – tai konkrečioms rizikos kategorijoms (pvz., operacinei, finansinei, atitikties), veiklos sritims, specifiniam turto vienetui ar turto grupei nustatyti leistini nukrypimai nuo bendro rizikos apetito, išreikšti kiekybinėmis ar kokybinėmis ribomis, kurių viršijimas reikalauja rizikos valdymo būdų taikymo. Pvz., jei organizacija nustato bendrą rizikos apetitą ir nusprendžia priimti rizikas iki vidutinio lygio, ji gali specifiniam IT infrastruktūros turtui nustatyti griežtesnę rizikos toleranciją ir priimti tik žemą riziką, atsižvelgdama į savo sektoriaus specifiką ir veiklos ypatumus.

Šios metodikos 5.3 priede pateiktas klausimynas ir 5.8 priede pateiktas rizikos profilių aprašas padės priimti sprendimus, kokius rizikos tolerancijos nukrypimus nuo bendro rizikos apetito rekomenduojama įvertinti.

Pavyzdys. UAB „LitBaltMed“ nustatė rizikos apetito ir tolerancijos kriterijus

UAB „LitBaltMed“ nustatė bendrą rizikos apetitą organizacijoje – priimti tik tas rizikas, kurių lygis žemas arba labai žemas. Vidutinio, aukšto ar labai aukšto lygio rizikos nėra laikomos priimtinomis. Tačiau atsižvelgdama į sveikatos priežiūros sektoriaus specifiką, jautrių pacientų duomenų tvarkymą ir į nacionalinius ir tarptautinius teisės aktus, reglamentuojančius rizikos valdymą, įmonė nusprendė nustatyti elektroninės medicininių duomenų ir receptų sistemos, kuri saugo ypač jautrius asmens sveikatos duomenis, rizikos tolerancijos lygį.

Įmonė nustatė elektroninės medicininių duomenų ir receptų sistemos griežtesnį rizikos tolerancijos lygį – toleruojama tik žema rizika. Tai reiškia, kad net jei kitos įmonės veiklos sritys ar turtai gali toleruoti vidutinio lygio riziką, pacientų duomenų sistemai taikomas žemesnis rizikos tolerancijos slenkstis ir pasiekus vidutinę riziką jau turi būti taikomos papildomos saugumo

3. Rizikos vertinimo procesas

3.1 Rizikos identifikavimas

Tai rizikos suradimo, atpažinimo ir aprašymo procesas, siekiant sudaryti rizikų, su kuriomis organizacija gali susidurti vykdydama savo veiklą, sąrašą.

Identifikuojant riziką, pirmiausia vertinamas turtas, tuomet priskiriamos aktualios grėsmės ir identifikuojami pažeidžiamumai, dėl kurių paveikiamas turtas.

Jeigu organizacija pageidauja taikyti kitokį rizikos identifikavimo metodą, pvz., grėsmių arba pažeidžiamumų pagrindo metodą, ji turi parengti ir patvirtinti pakeistą metodikos versiją.

3.1.1 Turto identifikavimas

Turto identifikavimas yra organizacijos turto vienetų ir grupių katalogo sudarymas ir jų vertinimas. Turto kataloge nurodomi rizikos vertinimui reikšmingi TIS turto vienetai ir grupės, žmogiškieji ištekliai ir organizacijos procesai.

Kiekviena organizacija sprendžia, kaip ir kokiu lygiu grupuojamas turtas. Didžioji dalis turto vienetų turėtų būti grupuojami, jei jų funkcija ir turto kritiškumas sutampa. Rekomenduojama informacinės sistemas (taikomoji programinė įranga) į katalogą įtraukti jų negrupuojant.

Jei organizacijoje anksčiau nebuvo identifikuotas turtas ir (ar) nebuvo sudarytas rizikos valdymo turto katalogas, tai turi būti padaryta šiame rizikos identifikavimo etape. Šis procesas taip pat turi būti atliktas, jei organizacijoje įvyko organizacinių pokyčių ar atsirado naujų turto vienetų ar grupių.

Standartinis turto katalogo šablonas pateiktas metodikos 5.4 priede. Organizacijoms privaloma šį katalogą pildyti pagal savo turimą turtą.

Dažniausiai turtą identifikuoja ir savo ekspertinę nuomonę teikia nustatant turto vienetus, grupes ir jų aspektus:

- turto savininkas (-ai);
- kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis;
- kibernetinio saugumo rizikos vertinimo ir valdymo specialistas.

Pavyzdys. UAB „LitBaltMed“ identifikavo organizacijos turto vienetus ir grupes.

UAB „LitBaltMed“ sudarė turto katalogą ir kiekvienam turto vienetui ar grupei nustatė priklausomybę nuo kito turto, tai, ar turtas pasiekiamas internetu, ir jo savininką.

Lentelėje nurodoma tik dalis organizacijos turto vienetų ir grupių.

Turto Nr.	Turto pavadinimas	Aprašymas / tikslas	Turto kategorija	Turto subkategorija	Matomas išorėje (Internete)	Turto/Proceso savininkas	Nuo kokio turto yra priklausomas šis turtas/procesas
Programinė_įrang							
T.PI. 1	Elektroninė medicininių duomenų ir receptų sistema (EMDRS)	Centralizuota pacientų duomenų ir elektroninių receptų valdymo sistema, sukurta ir prižiūrima išorės tiekėjo	Programinė_įranga	Taikomoji programinė įranga	Ne	Medicinos padalinio vadovas	T.PI.6, T.TI.1, T.TI.2, T.T.1, T.PE.3
T.PI. 8	Duomenų bazė „Oracle“	Duomenų bazė *Oracle* , veikianti kaip virtuali mašina *Hyper-V* aplinkoje, saugo pacientų medicinos įrašus, laboratorinius rezultatus ir sistemų duomenis	Programinė_įranga	Duomenų bazių valdymo sistemos	Ne	Medicinos padalinio vadovas	T.PI.6, T.PE.1
Techninė_įranga							
T.TI. 2	45 vnt. nešiojamų kompiuterių „Lenovo ThinkPad X1 Carbon Gen 9“	Kompiuteriai naudojami UAB „LitBaltMed“ darbuotojų administravimo darbams atlikti, medicininėms paslaugoms teikti ir organizacijos turtui valdyti (5 kompiuteriai laikomi atsargai)	Techninė_įranga	Nešiojamieji kompiuteriai	Ne	Informacinių technologijų administratorius	T.PI.11, T.PE.1, T.PE.3
T.TI. 3	Serveris „HP ProLiant DL380 Gen10“	Serveris, kuriame palaikomi UAB „LitBaltMed“ virtualizuoti serveriai	Techninė_įranga	Serveriai	Ne	Informacinių technologijų administratorius	T.PE.1
Tinklai							

3.1.1.1 Turto poveikio analizė

Turto vienetų ar grupių poveikio veiklai analizė atliekama siekiant nustatyti turto kritiškumo lygius. Šioje metodikoje turto kritiškumas vertinamas pagal konfidencialumo, vientisumo ir prieinamumo (angl. *confidentiality, integrity and availability*) aspektus. Analizė atliekama sudarant arba jau sudarius turto katalogą.

Kiekvienas kritiškumo aspektas vertinamas nuo 1 iki 5 balų, pagal tai, kokį poveikį vertinamo turto konfidencialumui, vientisumui ir prieinamumui turės incidentas:

- vertinant turto vieneto ar grupės konfidencialumą rekomenduojama atsižvelgti į tai, kokia informacija laikoma ir naudojama sistemoje ir kokios būtų šios informacijos paviešinimo pasekmės;
- vertinant turto vieneto ar grupės vientisumą rekomenduojama atsižvelgti į tai, kokia informacija perduodama, laikoma ar naudojama sistemoje, kokios kontrolės priemonės naudojamos informacijos vientisumui užtikrinti, kokios būtų pasekmės, jeigu informacija taptų netiksli ar neteisinga;
- vertinant prieinamumą rekomenduojama atsižvelgti į tai, per kiek laiko turi būti atnaujinta veikla, kokios organizacijos funkcijos priklauso nuo sistemos veikimo.

Turto kritiškumo lygis nustatomas pagal konfidencialumo, vientisumo ir prieinamumo balus. Didžiausias balas rodo turto kritiškumo lygį.

Kiti klausimai, pagal kuriuos galima nustatyti konfidencialumo, vientisumo ir prieinamumo lygį, pateikti klausimyne šios metodikos 5.3 priede.

Atliekant turto / veiklos poveikio analizę dažniausiai dalyvauja:

- turto savininkas (-ai);
- kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis;
- kibernetinio saugumo rizikos vertinimo ir valdymo specialistas.

Pavyzdys. UAB „LitBaltMed“ nustatė turto vienetų kritiškumo lygius.

UAB „LitBaltMed“ turto / veiklos poveikio įvertino turto vienetų ir grupių kritiškumo lygius.

Lentelėje nurodoma tik dalis organizacijos turto vienetų ir grupių.

Turto Nr.	Turto pavadinimas	Konfidencialumas	Vientisumas	Prieinamumas	Kritiškumas
Programinė_įrang					
T.PI. 1	Elektroninė medicininių duomenų ir receptų sistema (EMDRS)	5	4	3	5
T.PI. 8	Duomenų bazė „Oracle“	5	4	3	5
Techninė_įranga					
T.TI. 2	45 vnt. nešiojamų kompiuterių „Lenovo ThinkPad X1 Carbon Gen 9“	5	5	5	5
T.TI. 3	Serveris „HP ProLiant DL380 Gen10“	5	2	3	5
Tinklai					
T.T. 1	3 vnt. maršrutizatorių „Cisco RV340 Dual WAN Gigabit VPN Router“	5	5	3	5

3.1.2 Grėsmių identifikavimas

Grėsmių identifikavimas yra rizikos identifikavimo proceso etapas, kurio metu nustatomos organizacijai aktualios grėsmės, galinčios sukelti tam tikras pasekmes organizacijai arba organizacijos turtui.

Pagal šiuos šaltinius organizacija turi identifikuoti grėsmes, kurios gali kelti pavojų organizacijai:

- šios metodikos prieduose pateiktais grėsmių katalogais, veiklos sektorių rizikos profiliais ir klausimynu;
- tarptautinių ir nacionalinių kibernetinio saugumo organizacijų grėsmių ataskaitomis (ENISA, NKSC ir t. t.);
- bendradarbiavimo tarp veiklos sektoriaus organizacijų rezultatais;
- surinktais duomenimis (įvykusių incidentų, žinomų pažeidžiamumų ir t. t.).
- ekspertine nuomone.

Identifikuojant grėsmes svarbu įvertinti tik tas grėsmes, kurios reikšmingos nagrinėjamam turto vienetui ar grupei. Tai padeda išvengti perteklinio grėsmių vertinimo ir telkti dėmesį į svarbiausias rizikos sritis.

Dažniausiai grėsmes identifikuoja:

- turto savininkas (-ai);
- kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis;
- kibernetinio saugumo rizikos vertinimo ir valdymo specialistas.

Grėsmės identifikuojamos grupinėse diskusijose, taip pat naudojantis įvairiais ištekliais: grėsmių identifikavimo klausimynu (5.3 priedas), rizikos profiliais (5.8 priedas), pildomas grėsmių katalogas (5.6 priedas).

Grėsmių katalogas pateiktas metodikos 5.6 priede. Šis katalogas parengtas pagal standartus ISO/IEC 27005 ir „BSI-Standard 200-3“. Organizacijoms rekomenduojama šį sąrašą keisti pagal savo poreikius ir prioritetus.

Pavyzdys. UAB „LitBaltMed“ identifikavo grėsmes elektroninei medicininių duomenų ir receptų sistemai.

UAB „LitBaltMed“ identifikavo grėsmes, kurios daro ar gali daryti poveikį turto vienetui.

1	2	3	4	5	6
Rizikos identifikavimas					
Registro Nr.	Turto Nr.	Turto pavadinimas	Turto kategorija	Turto/Proceso savininkas(-ai)	Grėsmė
REG. 1	T.PI. 1	Elektroninė medicininių duomenų ir receptų sistema (EMDRS)	Programinė_įranga	Medicinos padalinio vadovas	Duomenų sugadinimas
REG. 2	T.PI. 1	Elektroninė medicininių duomenų ir receptų sistema (EMDRS)	Programinė_įranga	Medicinos padalinio vadovas	Neteisėtas asmens duomenų tvarkymas

3.1.3 Pažeidžiamumų identifikavimas

Pažeidžiamumų identifikavimas yra rizikos identifikavimo proceso etapas, kurio metu nustatomi turto vieneto ar grupės pažeidžiamumai, dėl kurių gali kilti grėsmės: atsirasti potencialios kibernetinio saugumo spragos, trūkumai ar neatitiktis reikalavimams.

Pažeidžiamumai vertinami pagal tai, kaip jie susiję su konkrečiu turtu ir konkrečia grėsme. Svarbu atkreipti dėmesį, kad pažeidžiamumų identifikavimas atliekamas rizikos identifikavimo procese, tuo pačiu metu kai turtui identifikuojamos grėsmės, siekiant nustatyti galimus pažeidžiamumus, kurie sudaro sąlygas grėsmei įvykti.

Pažeidžiamumų katalogas pateiktas metodikos 5.5 priede. Šis katalogas parengtas pagal dažniausiai nustatomus pažeidžiamumus. Organizacijoms rekomenduojama šį katalogą keisti pagal savo poreikius ir prioritetus, remiantis testavimo, audito rezultatais, turimu turtu, įvykusiais incidentais ir atsižvelgiant į priede 5.3. pateiktą klausimyną.

Remdamasi turimo turto ir aktualių grėsmių analizės rezultatais, organizacija įvertina, dėl kokių konkrečių pažeidžiamumų galėtų kilti grėsmės. Iš prieduose pateikto standartinių pažeidžiamumų katalogo atrenkami tik tie pažeidžiamumai, kurie gali pakenkti organizacijos turtui.

Dažniausiai pažeidžiamumus identifikuoja:

- turto savininkas(-ai);
- kibernetinio saugumo rizikos vertinimo ir valdymo specialistas;
- kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis.

Pavyzdys. UAB „LitBaltMed“ identifikavo elektroninės medicininių duomenų ir receptų sistemos pažeidžiamumus.

UAB „LitBaltMed“ indentifikavo pažeidžiamumus, susijusius su grėsmėmis, identifikuotomis praeitame etape.

1	2	3	4	5	6	7
Rizikos identifikavimas						
Registro Nr.	Turto Nr.	Turto pavadinimas	Turto kategorija	Turto/Proceso savininkas(-ai)	Grėsmė	Pažeidžiamumas
REG. 1	T.PI. 1	Elektroninė medicininių duomenų ir receptų sistema (EMDRS)	Programinė_įranga	Medicinos padalinio vadovas	Duomenų sugadinimas	PZ.39 - Nesaugi tinklo architektūra
REG. 2	T.PI. 1	Elektroninė medicininių duomenų ir receptų sistema (EMDRS)	Programinė_įranga	Medicinos padalinio vadovas	Neteisėtas asmens duomenų tvarkymas	PZ.16 - Neteisingas prieigos teisių suteikimas

3.1.4 Rizikų identifikavimas

Identifikavus kiekvieno turto vieneto ar grupės grėsmes ir pažeidžiamumus, aprašomos rizikos, susijusios su kiekvienu turtu. Rizika apibrėžiama kaip galimas nepageidaujamas įvykis, kai dėl nustatyto pažeidžiamumo kyla grėsmė konkrečiam turto vienetui ar grupei. Rizikos vertinamos pagal konkretų turto vienetą ar grupę.

Aprašant riziką, svarbu aiškiai identifikuoti potencialias jos priežastis, suprasti, kaip gali kilti konkreti grėsmė, kaip atsiranda specifinė rizika ir kokios sąlygos turi susidaryti ar veiksmai turi būti padaryti, kad rizika kiltų.

Rizikos registras yra sudedamoji rizikos valdymo įrankio dalis ir laikomas rizikos identifikavimo proceso rezultatu. Visos šiame registre užfiksuotos rizikos yra naudojamos tolesniuose rizikos analizės ir valdymo etapuose.

Organizacija turi registruoti identifikuotas rizikas į rizikos registrą. Rizikos registrai rengiami kiekvienam rizikos vertinimo ciklui. Rizikos registro šablonas su pavyzdžiu pateiktas 5.2 priede. Klausimynas, kuris padės identifikuoti aktualias rizikas, pateiktas 5.4 priede.

Pavyzdys. UAB „LitBaltMed“ nustatė ir aprašė elektroninės medicininių duomenų ir receptų sistemai kylančias rizikas.

UAB „LitBaltMed“ aprašė rizikas, nustatytas pagal praeituose etapuose identifikuotas grėsmes ir pažeidžiamumus.

1	2	3	4	5	6	7	8
Rizikos identifikavimas							
Registro Nr.	Turto Nr.	Turto pavadinimas	Turto kategorija	Turto/Proceso savininkas(-ai)	Grėsmė	Pažeidžiamumas	Rizikos aprašymas
REG. 1	T.PI. 1	Elektroninė medicininių duomenų ir receptų sistema (EMDRS)	Programinė_įranga	Medicinos padalinio vadovas	Duomenų sugadinimas	PZ.39 - Nesaugi tinklo architektūra	Darbuotojas atidaro kenkėjišką el. laišką savo darbo kompiuteryje. Dėl per mažo tinklo segmentavimo išpirkos programa plinta per ligoninės tinklą ir patenka į elektroninės medicininių duomenų ir receptų sistemos (EMDRS) serverį. Programa užšifruoja visus pacientų medicinos įrašus, receptų duomenis ir diagnostikos rezultatus.
REG. 2	T.PI. 1	Elektroninė medicininių duomenų ir receptų sistema (EMDRS)	Programinė_įranga	Medicinos padalinio vadovas	Neteisėtas asmens duomenų tvarkymas	PZ.16 - Neteisingas prieigos teisių suteikimas	Buvęs darbuotojas (atleistas dėl disciplinos pažeidimų), kuriam nebuvo laiku panaikintos prieigos teisės, keršydamas darbdaviui atsisiunčia tūkstančius pacientų įrašų ir paviešina juos internete.

3.1.5 Rizikos scenarijų rengimas

Organizacijoms, siekiančioms pažangesnio rizikos valdymo, rekomenduojama atlikus standartinius rizikos identifikavimo veiksmus, papildomai parengti rizikos scenarijus. Klausimus, kurie padėtų parengti rizikos scenarijus, pateikti 5.3 priede.

Dažniausiai rizikos scenarijus rengia:

- turto savininkas (-ai) – teikia savo ekspertizės rezultatus ir nurodo jo poveikį rengiant rizikos scenarijus;
- kibernetinio saugumo rizikos vertinimo ir valdymo specialistas – teikia savo ekspertizės rezultatus rizikos scenarijui parengti;
- kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis – kuria ir vertina rizikos scenarijus, remdamasis savo ekspertizės rezultatais.

3.2 Rizikos vertinimas

Šioje metodikoje taikomas kokybinis rizikos vertinimo metodas, išreikštas poveikio ir rizikos lygiu. Įvertinamos ankstesniame etape nustatytos rizikos ir nustatomi pirminis ir dabartinis rizikos lygiai. Tuo pačiu principu vertinamas ir galutinis rizikos lygis (3.3.2. skyrius).

3.2.1 Prigimtinio rizikos lygio nustatymas

Prigimtinis rizikos lygis nustatomas pagal kiekvienos rizikos poveikį ir tikimybę, nevertinant įdiegtų kontrolės priemonių. Kitose skyriuose pateikti kriterijai, pagal kuriuos galima nustatyti rizikos poveikio ir tikimybės lygius.

Prigimtinio rizikos lygį dažniausiai vertina:

- kibernetinio saugumo rizikos vertinimo ir valdymo specialistas – teikia savo ekspertizės rezultatus rizikos poveikiui ir tikimybei nustatyti;
- kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis – vertina rizikos poveikį ir tikimybę, remdamasis savo ekspertizės rezultatais.

3.2.1.1 Poveikio lygio nustatymas

Rizikos poveikio lygis nustatomas remiantis potencialios žalos kriterijais.

Kiekviena organizacija turi nusistatyti savo rizikos lygių kriterijus pagal žalos poveikį. Šioje metodikoje žala vertinama pagal 6 kriterijus, t. y.:

- finansiniai nuostoliai;
- veiklos tęstinumo sutrikimas;
- tiekimo grandinė;
- reputacija;
- teisinė atitiktis;
- žmogaus sveikata.

Organizacijai rekomenduojama pasirinkti jai aktualius kriterijus ir rizikos poveikį vertinti jais remiantis.

Organizacija turi sudaryti rizikos poveikio lentelę pagal rizikos kriterijus, aprašytus 2.2 skyriuje. Naudojantis šia lentele, kiekvienai rizikai priskiriamas poveikio lygis nuo „mažas“ (1) iki „katastrofinis“ (5). Identifikuotas poveikio lygis įrašomas į atitinkamą poveikio lygio stulpelį rizikos registre (5.2 priedas). Poveikio lentelės šablonas pateiktas 5.1 priede.

3.2.1.2 Tikimybės lygio nustatymas

Rizikos tikimybės lygis nustatomas pagal tai, kiek kartų tam tikra rizika kils arba atsiras per tam tikrą laiko tarpą.

Šioje metodikoje rizikos tikimybės lygiai nustatyti pagal tris kriterijus:

- įvykdymo paprastumo;
- įvykimo tikimybės;
- rizikos dažnio.

Rizikos tikimybę apskaičiuoti tiksliai yra labai sudėtinga, nes tikimybė nustatoma remiantis ekspertų nuomone, jau įvykusių incidentų duomenimis ir kibernetinio saugumo tendencijomis.

Rizikos tikimybės lygį taip pat galima nustatyti pagal tai, kaip lengva pažeidžiamumą aptikti, išnaudoti ir atkurti. Klausimai, kurie padės papildomai įvertinti šių rizikų tikimybę, pateikti 5.3 priede.

Pagal rizikos tikimybės lygio lentelę, pateiktą 5.1 priede, organizacija nustato tikimybės lygį nuo „mažai tikėtina“ (1) iki „neabejotina“ (5). Nustatytas tikimybės lygis įrašomas į atitinkamą tikimybės lygio stulpelį rizikos registre (5.2 priedas).

3.2.1.3 Prigimtinio rizikos lygio įvertinimas

Remiantis nustatytais poveikio ir tikimybės balais, kiekvienai rizikai priskiriamas lygis pagal poveikio ir tikimybės rizikos vertinimo lentelę. Rizikos lygis rodo, kokį pavojų organizacijai kelia tam tikra rizika.

Poveikio ir tikimybės rizikos vertinimo lentelė

Tikimybė	Poveikis				
	Mažas (1)	**Reikšmingas (2)**	**Rimtas (3)**	**Kritinis (4)**	**Katastrofinis (5)**
Neabejotina (5)	Maža	Vidutinė	Didelė	Labai didelė	Labai didelė
Labai tikėtina (4)	Maža	Vidutinė	Didelė	Didelė	Labai didelė
Tikėtina (3)	Maža	Vidutinė	Vidutinė	Didelė	Didelė
Mažai tikėtina (2)	Labai maža	Maža	Vidutinė	Vidutinė	Vidutinė
Reta (1)	Labai maža	Labai maža	Maža	Maža	Maža

Rizikos lygis	Balų diapazonas
Labai didelė	20–25
Didelė	11–19
Vidutinė	6–10
Maža	3–5
Labai maža	1–2

Rizikos registre rizikos lygis nustatomas pagal praeituose etapuose parinktas vertes.

Pavyzdys. UAB „LitBaltMed“ nustatė elektroninės medicininių duomenų ir receptų sistemai kylančios rizikos lygius.

UAB „LitBaltMed“ nustatė prigimtinį rizikos lygį nustatė elektroninės medicininių duomenų ir receptų sistemai kylančios rizikoms.

1	2	3	4	5	6	7
Rizikos identifikavimas						
Registro Nr.	Turto Nr.	Turto pavadinimas	Turto kategorija	Turto/Proceso savininkas(-ai)	Grėsmė	Pažeidžiamumas
REG. 1	T.PI. 1	Elektroninė medicininių duomenų ir receptų sistema (EMDRS)	Programinė_įranga	Medicinos padalinio vadovas	Duomenų sugadinimas	PZ.39 - Nesaugi tinklo architektūra
REG. 2	T.PI. 1	Elektroninė medicininių duomenų ir receptų sistema (EMDRS)	Programinė_įranga	Medicinos padalinio vadovas	Neteisėtas asmens duomenų tvarkymas	PZ.16 - Neteisingas prieigos teisių suteikimas

8	9	10	11
	Prigimtinės rizikos vertinimas		
Rizikos aprašymas	Prigimtinis rizikos poveikis	Prigimtinė rizikos tikimybė	Prigimtinis rizikos lygis
Darbuotojas atidaro kenkėjišką el. laišką savo darbo kompiuteryje. Dėl per mažo tinklo segmentavimo išpirkos programa plinta per ligoninės tinklą ir patenka į elektroninės medicininių duomenų ir receptų sistemos (EMDRS) serverį. Programa užšifruoja visus pacientų medicinos įrašus, receptų duomenis ir diagnostikos rezultatus.	5	4	20
Buvęs darbuotojas (atleistas dėl disciplinos pažeidimų), kuriam nebuvo laiku panaikintos prieigos teisės, keršydamas darbdaviui atsisiunčia tūkstančius pacientų įrašų ir paviešina juos internete.	5	2	10

3.2.2 Dabartinio rizikos lygio nustatymas

Dabartinio rizikos lygio nustatymas yra kiekvieno turto vieneto ar grupės jau įdiegtų kontrolės priemonių ir to, kaip jos pakeičia pirminį rizikos lygį, įvertinimas.

Dabartinį rizikos lygį dažniausiai nustato:

- turto savininkas (-ai);
- kibernetinio saugumo rizikos vertinimo ir valdymo specialistas;
- kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis.

3.2.2.1 Pritaikytų valdymo priemonių nustatymas

Šis procesas yra visų kontrolės priemonių, susijusių su vertinama rizika, nustatymas.

Pritaikytos valdymo priemonės identifikuojamos remiantis rizikos valdymo būdų aprašu (3.3.1 skyrius) ir rizikos valdymo priemonių katalogu (5.7 priedas). Identifikuotos kontrolės priemonės turi būti susijusios su nagrinėjamos rizikos grėsme ir pažeidžiamumais, net jei turtui apsaugoti pritaikyta daugiau valdymo priemonių.

Identifikuotos rizikos valdymo priemonės turi būti nurodomos atitinkamame rizikos registro stulpelyje (5.2 priedas).

Pavyzdys. UAB „LitBaltMed“, nustačiusi rizikas ir jų prigimtinius lygius, elektroninei medicininių duomenų ir receptų sistemai pritaikė rizikos valdymo priemones.

1	2	3	4	5	6	7	8	12
Rizikos identifikavimas								
Registro Nr.	Turto Nr.	Turto pavadinimas	Turto kategorija	Turto/Proceso savininkas(-ai)	Grėsmė	Pažeidžiamumas	Rizikos aprašymas	Jau pritaikytos rizikos valdymo priemonės
REG. 1	T.PI. 1	Elektroninė medicininių duomenų ir receptų sistema (EMDRS)	Programinė įranga	Medicinos padalinio vadovas	Duomenų sugadinimas	PZ.39 - Nesaugi tinklo architektūra	Darbuotojas atidaro kenkėjišką el. laišką savo darbo kompiuteryje. Dėl per mažo tinklo segmentavimo išpirkos programa plinta per ligoninės tinklą ir patenka į elektroninės medicininių duomenų ir receptų sistemos (EMDRS) serverį. Programa užšifruoja visus pacientų medicinos įrašus, receptų duomenis ir diagnostikos rezultatus.	VP. 142. Apsauga nuo kenkimo programų: kompiuterizuotuose darbo vietose įdiegtas „Microsoft Defender for Endpoint“ sprendimas su realaus laiko apsauga VP. 148. Informacijos atsarginės kopijos: išorinio tiekėjo teikiama atsarginių kopijų saugykla VP. 158. Saityno filtravimas: darbuotojų el. pašto dėžutės filtruoja laiškus
REG. 2	T.PI. 1	Elektroninė medicininių duomenų ir receptų sistema (EMDRS)	Programinė įranga	Medicinos padalinio vadovas	Neteisėtas asmens duomenų tvarkymas	PZ.16 - Neteisingas prieigos teisių suteikimas	Buvęs darbuotojas (atleistas dėl disciplinos pažeidimų), kuriam nebuvo laiku panaikintos prieigos teisės, keršydamas darbdaviui atsisiunčia tūkstančius pacientų įrašų ir paviešina juos internete.	-

3.2.2.2 Dabartinio rizikos lygio nustatymas

Identifikavus turto vieneto ar grupės kontrolės priemones, nustatomas įvertintų rizikų dabartinis lygis.

Pritaikius kontrolės priemones, rizikos poveikis ir tikimybė vertinami iš naujo.

Nustačius naują poveikio ir tikimybės lygį, nustatomas galutinis rizikos lygis ir nurodomas atitinkame galutinio rizikos lygio stulpelyje (5.2 priedas).

Pavyzdys. UAB „LitBaltMed“ nustatė elektroninei medicininių duomenų ir receptų sistemai kylančios rizikos dabartinį lygį.

UAB „LitBaltMed“ pritaikė rizikos valdymo priemones ir įvertino elektroninės medicininių duomenų ir receptų sistemai kylančios rizikos dabartinį lygį.

1	2	3	4	5	6	7	8
Rizikos identifikavimas							
Registro Nr.	Turto Nr.	Turto pavadinimas	Turto kategorija	Turto/Proceso savininkas(-ai)	Grėsmė	Pažeidžiamumas	Rizikos aprašymas
REG. 1	T.PI. 1	Elektroninė medicininių duomenų ir receptų sistema (EMDRS)	Programinė_įranga	Medicinos padalinio vadovas	Duomenų sugadinimas	PZ.39 - Nesaugi tinklo architektūra	Darbuotojas atidaro kenkėjišką el. laišką savo darbo kompiuteryje. Dėl per mažo tinklo segmentavimo išpirkos programa plinta per ligoninės tinklą ir patenka į elektroninės medicininių duomenų ir receptų sistemos (EMDRS) serverį. Programa užšifruoja visus pacientų medicinos įrašus, receptų duomenis ir diagnostikos rezultatus.
REG. 2	T.PI. 1	Elektroninė medicininių duomenų ir receptų sistema (EMDRS)	Programinė_įranga	Medicinos padalinio vadovas	Neteisėtas asmens duomenų tvarkymas	PZ.16 - Neteisingas prieigos teisių suteikimas	Buvęs darbuotojas (atleistas dėl disciplinos pažeidimų), kuriam nebuvo laiku panaikintos prieigos teisės, keršydamas darbdaviui atsisiunčia tūkstančius pacientų įrašų ir paviešina juos internete.

9	10	11	12	13	14	15
Prigimtinės rizikos vertinimas			**Dabartinės rizikos vertinimas**			
Prigimtinis rizikos poveikis	Prigimtinė rizikos tikimybė	Prigimtinis rizikos lygis	Jau pritaikytos rizikos valdymo priemonės	Dabartinis rizikos poveikis	Dabartinė rizikos tikimybė	Dabartinis rizikos lygis
5	4	20	VP. 142. Apsauga nuo kenkimo programų: kompiuterizuotuose darbo vietose įdiegtas „Microsoft Defender for Endpoint“ sprendimas su realaus laiko apsauga VP. 148. Informacijos atsarginės kopijos: išorinio tiekėjo teikiama atsarginių kopijų saugykla VP. 158. Saityno filtravimas: darbuotojų el. pašto dėžutės filtruoja laiškus	4	3	12
5	2	10	-	5	2	10

3.3 Rizikos valdymo būdų parinkimas

Parenkami kiekvienos rizikos valdymo būdai rizikos lygiui valdyti ir galutiniam lygiui apskaičiuoti.

3.3.1 Rizikos valdymo būdų parinkimas

Kiekvienai rizikai, viršijančiai rizikos apetitą arba rizikos toleranciją, turi būti pritaikytas vienas iš keturių rizikos valdymo būdų. Rizikos valdymo būdų veikimo principai:

- rizikos mažinimas;
- rizikos perdavimas;
- rizikos pašalinimas;
- rizikos priėmimas.

Šiame etape taip pat priskiriamas rizikos savininkas (-ai). Rizikos savininkas (-ai) yra vaidmuo ir atsakomybė, kuri priskiriama darbuotojui, turinčiam reikalingus ekspertizės duomenis ir pareigą valdyti ir stebėti riziką.

Dažniausiai rizikos valdymo būdus pritaiko:

- turto savininkas (-ai) (gali būti rizikos savininkas (-ai));
- kibernetinio saugumo rizikos vertinimo ir valdymo specialistas;
- kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis.

3.3.1.1 Rizikos mažinimas

Rizikos mažinimas yra rizikos valdymo būdas, kai rizikos lygis mažinamas rizikos valdymo priemonėmis. Tai gali būti nauja programinė įranga, pokyčiai organizacijos struktūroje ar infrastruktūroje, mokymai, naujos gerosios praktikos ar kiti metodai.

Rizikos mažinimo būdas pagrįstas rizikos poveikį ir / ar tikimybę iki organizacijai priimtino lygio mažinančių priemonių taikymu. Rizikos valdymo priemonės turi atitikti organizacijos finansines ir kitas galimybes ir nedaryti per didelės įtakos kitoms sistemoms.

Jei rizikos sumažinti nėra galimybės, nėra tinkamų rizikos valdymo priemonių ar potenciali žala mažesnė nei priemonių pritaikymo kaina, rekomenduojama taikyti kitus rizikos valdymo būdus.

Organizacija turi nustatyti rizikos valdymo priemones. Rizikos valdymo priemonių katalogas parengtas pagal ISO/IEC 27002 standartą ir dokumentą „CIS Critical Security Controls v8.0“, pateiktus 5.7.1 ir 5.7.2 prieduose.

Nustatytos rizikos valdymo priemones turi būti įrašomos į atitinkamą rizikos registre stulpelį (5.2 priedas).

3.3.1.2 Rizikos perdavimas

Rizikos perdavimas yra rizikos valdymo būdas, kai rizikos valdymas perduodamas trečiajai šaliai: tam tikros funkcijos perkėlimas, kibernetinio saugumo paslaugų užsakymas iš išorinio tiekėjo, draudimo sutarties sudarymas ar bet koks kitas būdas, kai rizikos lygio mažinimo principas priklauso nuo trečiosios šalies.

Rizikos perdavimas nepanaikina teisinės atsakomybės, todėl galutinė atsakomybė už riziką priskiriama organizacijai.

Rizikos perduodamos, kai:

- veiklos funkciją planuojama perduoti trečiajai šaliai;
- potenciali rizikos žala dažniausiai yra finansinio pobūdžio;
- yra prieinama paslauga, kuri adekvačiai sumažintų rizikos lygį;
- perduoti riziką išoriniam tiekėjui yra pigiau, negu pačiai organizacijai sumažinti rizikos lygį.

3.3.1.3 Rizikos vengimas

Rizikos vengimas yra rizikos valdymo būdas, kai atsisakoma su rizika susijusio turto ar funkcijų. Tai gali būti su rizika susijusio turto vieneto ar grupės nebenaudojimas ar tam tikros funkcijos sustabdymas, iki bus rastas kitas sprendimas.

Rizikos vengimo būdas pasirenkamas tada, kai:

- nėra įdiegiamų rizikos valdymo priemonių arba jos per brangios, tačiau rizika per didelė, kad ją būtų galima priimti;
- pritaikius rizikos valdymo priemones sistema tampa per sudėtinga (labai sudėtinga arba kompleksiška).

3.3.1.4 Rizikos priėmimas

Rizikos priėmimas – tai sprendimas prisiimti riziką be jokių rizikos valdymo būdų ar rizikos lygio mažinimo priemonių.

Rizikos priėmimo būdas pasirenkamas tada, kai:

- rizika pakankamai maža, kad ją būtų galima priimti be papildomų kontrolės priemonių;
- rizikos valdymo priemonių kaina didesnė nei turto vieneto ar grupės vertė ar potenciali rizikos finansinė žala;
- organizacija neturi išteklių rizikos valdymo priemonėms įdiegti;
- nėra įdiegiamų rizikos valdymo priemonių;
- funkcija arba turto vienetas ar grupė yra per svarbūs, kad būtų galima jų atsisakyti, ir organizacija neturi išteklių rizikos valdymo priemonėms įdiegti.

Pavyzdys. UAB „LitBaltMed“ parinko elektroninės medicininių duomenų ir receptų sistemai kylančios rizikos valdymo būdus ir priemones.

UAB „LitBaltMed“ elektroninės medicininių duomenų ir receptų sistemai kylančiai rizikai buvo paskirti savininkai, parinkti rizikos valdymo būdai ir priemonės.

1	2	3	4	5	6	7	8	12	18
Rizikos identifikavimas								Dabartinės rizikos vertinimas	Rizikos valdymo būdų parinkimas
Registro N	Turto N	Turto pavadinima	Turto kategorija	Turto/Proceso savininkas(-ai)	Grėsmė	Pažeidžiamumas	Rizikos aprašymas	Jau pritaikytos rizikos valdymo priemonės	Rizikos valdymo būdo ir priemonių aprašymas
REG. 1	T.PI. 1	Elektroninė medicininių duomenų ir receptų sistema (EMDRS)	Programinė_įranga	Medicinos padalinio vadovas	Duomenų sugadinimas	PZ.39 - Nesaugi tinklo architektūra	Darbuotojas atidaro kenkėjišką el. laišką savo darbo kompiuteryje. Dėl per mažo tinklo segmentavimo išpirkos programa plinta per ligoninės tinklą ir patenka į elektroninės medicininių duomenų ir receptų sistemos (EMDRS) serverį. Programa užšifruoja visus pacientų medicinos įrašus, receptų duomenis ir diagnostikos rezultatus.	VP. 142. Apsauga nuo kenkimo programų: kompiuterizuotuose darbo vietose įdiegtas „Microsoft Defender for Endpoint“ sprendimas su realaus laiko apsauga VP. 148. Informacijos atsarginės kopijos: išorinio tiekėjo teikiama atsarginių kopijų saugykla VP. 158. Saityno filtravimas: darbuotojų el. pašto dėžutės filtruoja laiškus	VP. 157. Tinklų atskyrimas: atskirti EMDRS serverį į atskirą tinklo segmentą (VLAN) mikrosegmentacijos principais VP. 144. Konfigūracijų valdymas: nustatyti saugiasienių, ribojančių prieigą prie EMDRS, naudojimo taisykles
REG. 2	T.PI. 1	Elektroninė medicininių duomenų ir receptų sistema (EMDRS)	Programinė_įranga	Medicinos padalinio vadovas	Neteisėtas asmens duomenų tvarkymas	PZ.16 - Neteisingas prieigos teisių suteikimas	Buvęs darbuotojas (atleistas dėl disciplinos pažeidimų), kuriam nebuvo laiku panaikintos prieigos teisės, keršydamas darbdaviui atsisiunčia tūkstančius pacientų įrašų ir paviešina juos internete.	-	VP. 147. Duomenų nutekinimo prevencija: "Microsoft Windows Directory" įjungta konfigūracija, neleidžianti duomenų perkelti į nepatvirtintus įrenginius, fizines ir debesų duomenų laikmenas

3.3.2 Galutinio rizikos lygio nustatymas

Galutinis rizikos lygis rodo rizikos keliamą pavojų organizacijai, kai bus pritaikyti rizikos valdymo būdai ir priemonės.

Galutinis rizikos lygis apskaičiuojamas pagal dabartinį rizikos lygį, vertinant, kaip pasikeis rizikos poveikis ir (ar) tikimybė pritaikius rizikos valdymo būdus. Tada galutinis rizikos lygis apskaičiuojamas pagal poveikio ir tikimybės rizikos lentelę ir įrašomas į rizikos registrą (5.2 priedas).

Jei įvertinus galutinį rizikos lygį, jis išlieka virš organizacijos rizikos apetito, rizikos savininkas turi pakartoti praeitą žingsnį, su tikslu sumažinti rizikos lygį iki organizacijos apetito lygio.

Galutinį rizikos lygį dažniausiai nustato:

- rizikos savininkas (-ai);
- kibernetinio saugumo rizikos vertinimo ir valdymo specialistas;
- kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis.

Pavyzdys. UAB „LitBaltMed“ įvertino elektroninės medicininių duomenų ir receptų sistemai kylančios rizikos galutinį lygį.

Pagal parinktus rizikos valdymo būdus ir priemones elektroninės medicininių duomenų ir receptų sistemos rizikų poveikis ir tikimybė buvo įvertinti iš naujo ir nustatytas galutinis rizikos lygis. Rizikos „REG.2“ galutinis lygis nustatytas pagal rizikos apetito ir tolerancijos ribas (balas <6, t. y. labai mažas arba mažas rizikos lygis), tačiau rizikos „REG. 1“ lygis viršija rizikos tolerancijos EMDRS ribas (balas >=6, t. y. vidutinis, didelis ir labai didelis rizikos lygis).

1	2	3	4	5	6	7	8	9	10	11
Rizikos identifikavimas								Prigimtinės rizikos vertinimas		
Registro Nr	Turto Nr	Turto pavadinimas	Turto kategorija	Turto/Proceso savininkas(-ai)	Grėsmė	Pažeidžiamumas	Rizikos aprašymas	Prigimtinis rizikos poveikis	Prigimtinė rizikos tikimybė	Prigimtinis rizikos lygis
REG. 1	T.PI. 1	Elektroninė medicininių duomenų ir receptų sistema (EMDRS)	Programinė įranga	Medicinos padalinio vadovas	Duomenų sugadinimas	PZ.39 - Nesaugi tinklo architektūra	Darbuotojas atidaro kenkėjišką el. laišką savo darbo kompiuteryje. Dėl per mažo tinklo segmentavimo išpirkos programa plinta per ligoninės tinklą ir patenka į elektroninės medicininių duomenų ir receptų sistemos (EMDRS) serverį. Programa užšifruoja visus pacientų medicinos įrašus, receptų duomenis ir diagnostikos rezultatus.	5	4	20
REG. 2	T.PI. 1	Elektroninė medicininių duomenų ir receptų sistema (EMDRS)	Programinė įranga	Medicinos padalinio vadovas	Neteisėtas asmens duomenų tvarkymas	PZ.16 - Neteisingas prieigos teisių suteikimas	Buvęs darbuotojas (atleistas dėl disciplinos pažeidimų), kuriam nebuvo laiku panaikintos prieigos teisės, keršydamas darbdaviui atsisiunčia tūkstančius pacientų įrašų ir paviešina juos internete.	5	2	10

12	13	14	15	16	17	18	19	20	21
	Dabartinės rizikos vertinimas			Rizikos valdymo būdų		Rizikos valdymo būdų parinkimas			
Jau pritaikytos rizikos valdymo priemonės	Dabartinis rizikos poveikis	Dabartinė rizikos tikimybė	Dabartinis rizikos lygis	Rizikos savininkas(-ai)	Rizikos valdymo būdas	Rizikos valdymo būdo ir priemonių aprašymas	Galutinis rizikos poveikis	Galutinė rizikos tikimybė	Galutinis rizikos lygis
VP. 142. Apsauga nuo kenkimo programų: kompiuterizuotuose darbo vietose įdiegtas „Microsoft Defender for Endpoint“ sprendimas su realaus laiko apsauga VP. 148. Informacijos atsarginės kopijos: išorinio tiekėjo teikiama atsarginių kopijų saugykla VP. 158. Saityno filtravimas: darbuotojų el. pašto dėžutės filtruoja laiškus	4	3	12	Kibernetinio sagumo vadovas ir (ar) saugos įgaliotinis	Rizikos mažinimas	VP. 157. Tinklų atskyrimas: atskirti EMDRS serverį į atskirą tinklo segmentą (VLAN) mikrosegmentacijos principais VP. 144. Konfigūracijų valdymas: nustatyti saugiasienių, ribojančių prieigą prie EMDRS, naudojimo taisykles	4	2	8
-	5	2	10	Informacinių technologijų administratorius	Rizikos mažinimas	VP. 147. Duomenų nutekinimo prevencija: "Microsoft Windows Directory" įjungta konfigūracija, neleidžianti duomenų perkelti į nepatvirtintus įrenginius, fizines ir debesų duomenų laikmenas	2	1	2

3.3.3 Rizikos valdymo plano sudarymas

Atlikus rizikos vertinimą ir parinkus konkrečius rizikos valdymo būdus ir priemones, turi būti sudaromas rizikos valdymo planas. Šiame plane turi būti nurodomi visi rizikos mažinimo, perdavimo, šalinimo būdai ir pateikiamas rizikos valdymo procesų eiliškumas pagal skubą.

Į rizikos valdymo planą įtraukiamos tik tos rizikos, kurioms vertinimo metu buvo parinktos valdymo priemonės, nepriklausomai nuo pasirinktos strategijos (mažinimo, perdavimo ar šalinimo). Rizikos, kurios vertinimo metu buvo sąmoningai priimtos (toleruojamos) arba dėl kurių neplanuojama imtis jokių veiksmų, plane nedetalizuojamos – jos lieka rizikos registre stebėsenai vykdyti.

Į valdymo planą turėtų būti įtrauktos šios dalys:

- kiekvienos rizikos valdymo sprendimo pagrindimas;
- planuojami veiksmai ir jų įgyvendinimo terminai;
- atsakingi asmenys (valdymo priemonės įgyvendintojas ir atsakingas asmuo už įgyvendinimo stebėseną);
- reikalingi resursai ir biudžetas;
- kiekvieno veiksmo būsena (nepradėta, vykdoma, užbaigta).

Parengtą planą kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis pristato organizacijos vadovybei. Prieš organizacijos vadovybei patvirtinant planą, suplanuojamas atitinkamas biudžetas, sudaromi įgyvendinimo grafikai ir numatomi reikalingi ištekliai.

Vadovybės patvirtinto plano įgyvendinimas turi būti stebimas, o pažanga – fiksuojama. Rizikos savininkai kartu su kibernetinio saugumo vadovu ir (ar) saugos įgaliotiniu yra atsakingi už plano vykdymą ir efektyvumą.

Standartinis rizikos valdymo planas pateikiamas 5.9 priede.

Rizikos valdymo planą dažniausiai sudaro:

- rizikos savininkas(-ai);
- kibernetinio saugumo rizikos vertinimo ir valdymo specialistas;
- kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis.

Pavyzdys. UAB „LitBaltMed“ sudarė rizikos valdymo planą.

UAB „LitBaltMed“ elektroninės medicininių duomenų ir receptų sistemai kylančiai rizikai nustatyti valdymo terminai ir apsvarstyti reikalingi ištekliai ir biudžetas. Svarbu paminėti, kad biudžeto langeliai tušti, nes šiems rizikos valdymo būdams ir priemonėms nereikalinga papildoma įranga ar investicijos.

Rizikos registro Nr.	Rizikos aprašymas	Prigimtinis rizikos lygis	Dabartinis rizikos lygis	Galutinis rizikos lygis	Rizikos valdymo būdas	Rizikos valdymo būdo ir priemonių aprašymas
REG. 1	Darbuotojas atidaro kenkėjišką el. laišką savo darbo kompiuteryje. Dėl per mažo tinklo segmentavimo išpirkos programa plinta per ligoninės tinklą ir patenka į elektroninės medicininių duomenų ir receptų sistemos (EMDRS) serverį. Programa užšifruoja visus pacientų medicinos įrašus, receptų duomenis ir diagnostikos rezultatus.	20	12	8	Rizikos mažinimas	VP. 157. Tinklų atskyrimas: atskirti EMDRS serverį į atskirą tinklo segmentą (VLAN) mikrosegmentacijos principais VP. 144. Konfigūracijų valdymas: nustatyti saugiasienių, ribojančių prieigą prie EMDRS, naudojimo taisykles
REG. 2	Buvęs darbuotojas (atleistas dėl disciplinos pažeidimų), kuriam nebuvo laiku panaikintos prieigos teisės, keršydamas darbdaviui atsisiunčia tūkstančius pacientų įrašų ir paviešina juos internete.	10	10	2	Rizikos mažinimas	VP. 147. Duomenų nutekinimo prevencija: "Microsoft Windows Directory" įjungta konfigūracija, neleidžianti duomenų perkelti į nepatvirtintus įrenginius, fizines ir debesų duomenų laikmenas

Turto/Proceso savininkas(-ai)	Rizikos savininkas	Reikalingi resursai	Reikalingas biudžetas	Biudžetas	Įgyvendinimo terminas	Rizikos valdymo etapas
Medicinos padalinio vadovas	Kibernetinio sagumo vadovas ir (ar) saugos įgaliotinis	3 žmogaus dienos	0 €	Patvirtinta	2025 K4	Planavimas
Medicinos padalinio vadovas	Informacinių technologijų administratorius	5 žmogaus dienos	0 €	Patvirtinta	2025 K3	Planavimas

3.4 Rizikos stebėsena ir informavimas

Paskutinis rizikos valdymo proceso etapas yra rizikos stebėjimas ir informavimas apie ją. Šis etapas trunka iki kito rizikos valdymo proceso pradžios. Proceso metu stebimi pokyčiai organizacijoje, organizacijos pažeidžiamumas ir rizikos valdymo būdų pritaikymo efektyvumas ir vertinamas pats rizikos valdymo procesas.

3.4.1 Organizacijos pokyčių stebėjimas

Organizacijoje įvykus vidiniams pokyčiams, gali pasikeisti organizacijos rizikos atlaikymo pajėgumas, apetitas kibernetinio saugumo rizikoms. Šie pokyčiai gali būti:

- organizacijos TIS infrastruktūros pokyčiai;
- naujų funkcijų sukūrimas;
- tiekimo grandinės pokyčiai;
- įstatymų, susijusių su organizacija, pokyčiai.

Įvykus pokyčiams, organizacija turi įvertinti, ar rizikos valdymo metodika atitinka organizacijos poreikius ir rizikos kriterijus, ir jei reikia atnaujinti ir patvirtinti naują rizikos valdymo tvarką.

Rizikos stebėjimo ir informavimo procese dažniausiai dalyvauja kibernetinio saugumo vadovas ir (ar) jo įgaliotinis – stebi pokyčius organizacijoje ir yra informuojamas apie juos, vertina, kada ir kokie pokyčiai reikalingi organizacijos rizikos valdymo dokumentacijoje ir procese, bei įgyvendina šiuos pokyčius.

3.4.2 Grėsmių žvalgyba

Kibernetinio saugumo grėsmių ir pažeidžiamumų aplinka (angl. *threat landscape*) nuolat keičiasi ir tam tikros grėsmės gali tapti pavojingesnės ar dažnesnės, gali kilti naujų grėsmių – tai kelia pavojų organizacijos veiklai ir daro ją dar pažeidžiamesnę.

Grėsmės žvalgyba (angl. *threat intelligence*) yra grėsmių ir pažeidžiamumų stebėjimas. Grėsmės žvalgybą rekomenduojama atlikti kiekvienai organizacijai. Dėl stebėjimo pobūdžio (tai reikalauja išteklių) ne visoms organizacijoms tai įmanoma. Paprastesnis, tačiau mažiau efektyvus būdas grėsmių žvalgybą atlikti remiantis tarptautinių ir nacionalinių kibernetinio saugumo organizacijų publikacijomis ir ataskaitomis. Grėsmės žvalgybą gali atlikti išorinis tiekėjas.

Grėsmių žvalgybą dažniausiai atlieka kibernetinio saugumo vadovas ir (ar) jo įgaliotinis. Jis stebi kibernetinio saugumo grėsmių ir pažeidžiamumų aplinką ir bando nustatyti, kaip tai susiję su organizacija ir įgyvendina reikalingus pokyčius organizacijos rizikos valdymo dokumentacijoje ir procese.

3.4.3 Rizikos valdymo būdų pritaikymo stebėjimas

Patvirtinus rizikos valdymo planą, procesą reikia stebėti, kad rizikos valdymo būdus ir priemones būtų galima pritaikyti laiku ir rasti sprendimus susidūrus su kliūtimis.

Dažniausiai rizikas stebi ir apie jas informuoja:

- rizikos savininkas(-ai) – praneša apie progresą, kai pritaikomi rizikos valdymo būdai ir priemonės, taip pat nurodo priežastis, jei rizikos valdymo būdai ir priemonės nepritaikomos laiku;
- kibernetinio saugumo vadovas ir (ar) jo įgaliotinis – teikia savo ekspertizės, atliktos dėl sprendimų priėmimo susidūrus su kliūtimis, rezultatus, tikrina būdų ir priemonių pritaikymo progresą ir rezultatus praneša vadovybei.

3.4.4 Rizikos stebėjimo rodiklių nustatymas

Siekiant užtikrinti objektyvų ir efektyvų rizikos valdymo proceso, pritaikytų rizikos valdymo būdų ir priemonių stebėjimą, šioje metodikoje remiamasi stebėsenos rodikliai ir rizikos indikatoriai.

Rodikliai nustatomi pagal tai, kokios pobūdžio yra su rizika susijusi grėsmė, ir taikomi tik objektyviai matuojamiems dydžiams. Šis matmuo gali būti:

- skaičius (incidentų, nesėkmingų prisijungimo bandymų skaičius);
- santykis (kiek procentų visos techninės įrangos turi naujausią programinę įrangą);
- matavimo vienetai (prastovos skaičius valandomis, nuostoliai eurais).

Dažniausiai rizikas stebi ir apie jas informuoja:

- turto savininkas (-ai) (gali būti rizikos savininkas (-ai));
- rizikos savininkas (-ai) (gali būti turto savininkas (-ai));
- kibernetinio saugumo rizikos vertinimo ir valdymo specialistas;
- kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis.

3.4.4.1 Stebėsenos rodikliai

Stebėsenos rodikliai (angl. *key performance indicators*, KPI) naudojami rizikos valdymo būdų ir priemonių efektyvumui įvertinti. Šiuos rodiklius rekomenduojama naudoti visoms rizikoms, kurios vertinimo metu viršijo organizacijos rizikos apetitą ar toleranciją, prieš pritaikant rizikos valdymo būdus ir kurių stebėjimas ir matavimas suteikia reikšmingos informacijos.

Stebėsenos rodiklis rodo pritaikyto rizikos valdymo būdo ar priemonių efektyvumą, kai lyginamas rodiklis prieš ir po rizikos valdymo būdo ar priemonės pritaikymo. Kiekvienas stebėsenos rodiklis turėtų būti parinktas taip, kad jo dydis būtų tiesiogiai susijęs su stebima rizika, ir matmens pokyčiai tiesiogiai atspindėtų rizikos pokyčius.

3.4.4.2 Rizikos indikatoriai

Rizikos indikatoriai (angl. *key risk indicators* / KRIs) yra rodikliai, kurie nurodo organizacijos pažeidžiamumą ir pokyčius. Jie naudojami organizacijai aktualioms grėsmėms ir rizikoms stebėti.

Rizikos indikatorių veikimo principas yra pagrįstas nuolatiniu matuojamų dydžių stebėjimu ir dabartinių duomenų lyginimu su ankstesniais duomenimis. Reikšmingi stebimų dydžių skirtumai rodo, kad rizikos poveikis arba tikimybė pasikeičia.

Į gautų išvadų duomenis turi būti atsižvelgiama atliekant kitą rizikos vertinimą arba rizikos vertinimas pradedamas *ad hoc* principu.

Pavyzdys. UAB „LitBaltMed“ nustatė stebėsenos rodiklius ir rizikos indikatorius

Stebėsenos rodiklis

UAB „LitBaltMed“, nustačiusi *fišingo* atakų riziką, testuoja ir rengia kibernetinio saugumo mokymus, kuriuos vykdo išorinis tiekėjas. Šio testavimo efektyvumui stebėti taiko rodiklį –darbuotojų, kurie paspaudė nuorodą *fišingo* laiške prieš ir po kibernetinio saugumo mokymų, skaičių.

Skaičius darbuotojų, kurie paspaudė nuorodą testavimo laiške:

- mažas – ≤5 % darbuotojų (iki 2 darbuotojų);
- vidutinis – >5 %, ≤10 % darbuotojų (nuo 3 iki 4 darbuotojų);
- didelis – >10 % darbuotojų (daugiau kaip 4 darbuotojai).

Šis rodiklis rodo, kiek darbuotojų yra atsparūs *fišingo* atakoms.

Rizikos indikatorius:

UAB „LitBaltMed“ nustatė kelias rizikas, susijusias su kibernetinėmis prieigos teisių išgavimo atakomis. Organizacija nustatė šios rizikos rodiklį – nesėkmingų prisijungimų atvejų skaičių per mėnesį.

Nesėkmingų prisijungimų atvejų skaičius per mėnesį. Įprastas neteisingų prisijungimų atvejų skaičius – <3200 prisijungimų atvejų skaičius per mėnesį.

Šis rodiklis rodo galimus bandymus įsilaužti į sistemą mėginant atspėti paskyrų slaptažodžius, o reikšmingas neteisingų prisijungimų atvejų skaičiaus didėjimas gali perspėti apie naujus pažeidžiamumus ar atakas.

4. Vartojamos sąvokos

Ad hoc - tai neplanuotas, vienkartinis veiksmas ar sprendimas, atliekamas atsiradus konkrečiam poreikiui. Kibernetinio saugumo kontekste tai reiškia rizikos vertinimą ar veiksmą, inicijuotą reaguojant į netikėtą situaciją, o ne pagal nustatytą grafiką.

Atitikties pareigūnas – tai darbuotojas, atsakingas už tai, kad organizacijos veikla atitiktų taikomus įstatymus, reglamentus ir vidines politikos nuostatas. Jis atlieka priežiūrą ir teikia rekomendacijas dėl procesų tobulinimo, siekdamas užtikrinti teisinių reikalavimų laikymąsi.

Auditas – tai nepriklausomas, sistemingas ir dokumentuotas organizacijos procesų, priemonių ar veiklos aspektų vertinimas, atliekamas siekiant nustatyti, ar jis atitinka nustatytus reikalavimus, vidaus taisykles, standartus ar gerąsias praktikas.

Dabartinė rizika – tai rizika, kuri lieka įvertinus jau pritaikytus rizikos valdymo būdus ir priemones. Ji rodo, kiek organizacija šiuo metu yra apsaugota nuo konkrečių grėsmių, atsižvelgiant į jau pritaikytų rizikos valdymo būdų ir priemonių efektyvumą.

Esminis subjektas – tai kibernetinio saugumo subjektas, įtrauktas į Kibernetinio saugumo informacinės sistemos (KSIS) Kibernetinio saugumo subjektų (KSS) registrą ir atitinkantis specialiuosius kriterijus, nustatytus pagal Lietuvos Respublikos kibernetinio saugumo įstatymą ir NIS2 direktyvą.

Galutinė rizika – tai rizika, kuri lieka pritaikius rizikos valdymo būdus ir priemones, atsižvelgiant į organizacijos nustatytą rizikos tolerancijos ir priimtinumo lygį.

Grėsmė – tai potencialus įvykis ar veiksnys, kuris gali sukelti neigiamą poveikį organizacijos turtui, veiklos procesams ar informacijos saugumui, pasireiškiantis sąmoninga (pvz., kibernetinė ataka) ar atsitiktine (pvz., įrangos gedimas) forma.

Kibernetinio saugumo rizika – tai tikimybė, kad tam tikras įvykis ar veiksnys turės neigiamą poveikį organizacijos tikslams, veiklos tęstinumui ar turtui.

Kibernetinio saugumo turto ir rizikos identifikavimas – tai veiksmas, kurio metu nustatomas svarbus organizacijos turtas, su juo susijusios grėsmės ir pažeidžiamumai. Tai būtina pradinė sąlyga rizikos analizei atlikti.

Kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis – tai organizacijoje paskirtas asmuo arba asmenys, atsakingi už tinklų ir informacinių sistemų atitikties Lietuvos Respublikos kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams užtikrinimą ir kitų teisės aktuose nustatytų funkcijų vykdymą.

Organizacijos masto rizikos vertinimas – tai visos organizacijos mastu atliekamas rizikos nustatymas, analizė ir vertinimas. Jo tikslas – įvertinti sistemines rizikas, bendrus pažeidžiamumus ir jų poveikį visos organizacijos kritinėms funkcijoms, kitaip nei atliekant kibernetinio saugumo rizikos vertinimą, kuris apima specifines IT ir informacinių sistemų grėsmes.

Organizacijos vadovybė – tai aukščiausio lygmens organizacijos valdymo subjektas, atsakingas už strateginių tikslų formavimą, sprendimų priėmimą ir išteklių paskirstymą. Ji užtikrina organizacijos veiklos kryptingumą, priežiūri valdymo sistemų įgyvendinimą ir palaiko esminius sprendimus įvairiose srityse, įskaitant kibernetinį saugumą. Vadovybė taip pat prisiima teisinę atsakomybę už organizacijos valdomos informacijos apsaugą.

Pažeidžiamumas – tai sistemos, proceso ar organizacijos silpnoji vieta kuri gali būti išnaudota grėsmių poveikiui atsirasti arba padidinti rizikos įtaką informacijos saugumui, veiklos tęstinumui ar kitoms kritinėms funkcijoms.

Prigimtinė rizika – tai rizikos lygis, kuris egzistuotų, jei nebūtų taikomi jokie rizikos valdymo būdai ir priemonės. Ji atspindi grėsmių ir pažeidžiamumų poveikį organizacijos turtui ir veiklai, kai jie visiškai neapsaugoti.

Rizikos apetitas tai rizikos priimtinumo dydis, kurį organizacija yra pasirengusi prisiimti ir kurį viršijančioms rizikoms turi būti taikomi rizikos valdymo būdai.

Rizikos atlaikymo pajėgumas – tai organizacijos pajėgumas valdyti rizikos poveikį nepažeidžiant esminių veiklos tikslų ir finansinio stabilumo. Jis priklauso nuo turimų išteklių, infrastruktūros atsparumo, rizikos valdymo mechanizmų ir organizacinės brandos.

Rizikos konteksto ir kriterijų nustatymas – tai etapas, kuriame apibrėžiama rizikos vertinimo apimtis, tikslai, atlaikymo pajėgumas, apetitas ir tolerancija.

Rizikos lygis – rizikos pavojingumo matmuo nuo „labai mažas“ (1) iki „katastrofinis“ (5). Rizikos lygis nustatomas pagal rizikos poveikio ir tikimybės lygius.

Rizikos mažinimas – rizikos valdymo būdas, kai įgyvendinamos priemonės siekiant sumažinti rizikos tikimybę ar poveikį iki lygio, atitinkančio organizacijos rizikos apetitą.

Rizikos perdavimas – rizikos valdymo būdas, kai atsakomybė už rizikos valdymą perleidžiama išorės subjektui, pavyzdžiui, paslaugų tiekėjui ar draudimo bendrovei, taip mažinant rizikos poveikį organizacijos veiklai rizikos apetito ribose.

Rizikos priėmimas – rizikos valdymo būdas, kai organizacija sąmoningai toleruoja esamą rizikos lygį, nepriklausomai nuo to, ar jis atitinka nustatytą rizikos apetitą. Tokiu atveju papildomos valdymo priemonės netaikomos, o sprendimas priimamas įvertinus galimą poveikį, sąnaudas ir alternatyvų nebuvimą.

Rizikos registras – tai dokumentas ar sistema, kurioje fiksuojamos identifikuotos rizikos, jų vertinimai ir stebėsenos duomenys. Jis padeda centralizuotai valdyti rizikos informaciją.

Rizikos savininkas (-ai) – rizikos savininkas yra asmuo ar padalinys, kuris atsakingas už konkrečios rizikos valdymą ir stebėseną, paskiriamas rizikos valdymo būdų ir priemonių rinkimo etape. Jis vykdo priimtus sprendimus dėl rizikos valdymo būdų ir priemonių ir jų pritaikymo.

Rizikos scenarijus – tai struktūruotas galimos grėsmės vystymosi modelis nuo priežasties iki poveikio. Scenarijus padeda tiksliau įvertinti rizikos poveikį, tikimybę ir reikalingus rizikos valdymu būdus ir priemones.

Rizikos stebėjimas ir informavimas – tai procesas, apimantis rizikos būklės sekimą ir informacijos pateikimą suinteresuotiems asmenims. Tokiu būdu užtikrinama sprendimų priėmimo pagrįstumas.

Rizikos stebėsena – tai nuolatinis procesas, kurio metu vertinamas įgyvendintų rizikos valdymo būdų ir priemonių veiksmingumas. Stebėsena leidžia laiku nustatyti naujas rizikas ar esamos rizikos pokyčius.

Rizikos tolerancija – tai konkrečioms rizikos kategorijoms (pvz., operacinė, finansinė, atitikties) ar veiklos sritims ar specifiniam turtui ar turto grupei nustatyti leistini nukrypimai nuo bendro rizikosapetito, išreikšti kiekybiniais ar kokybiniais limitais, kuriuos viršijant būtina parinkti rizikos valdymo būdus ir priemones.

Rizikos valdymas – tai sistemingas ir nuolat pasikartojantis rizikos nustatymo, vertinimo, planavimo, įgyvendinimo ir kontrolės procesas, kurį sudaro visuma organizacijos nustatytų ir taikomų principų, strategijų, politikų, vidaus procedūrų, valdysenos, komunikacijos kanalų, jos vadovų, pagrindines funkcijas atliekančių asmenų ir darbuotojų kompetencija ir jų dalyvavimas veiklos, įskaitant ir su ja susijusių rizikų, valdymo procese.

Rizikos vengimas – rizikos valdymo būdas, kai eliminuojamas pats rizikos šaltinis, dažniausiai atsisakant tam tikros veiklos, proceso ar technologijos, kuriai kylanti rizika viršija organizacijos rizikos apetitą.

Svarbus subjektas – tai kibernetinio saugumo subjektas, įtrauktas į Kibernetinio saugumo subjektų registrą, kuris atitinka bendruosius ir (ar) specialiuosius identifikavimo kriterijus, nustatytus Kibernetinio saugumo įstatyme.

Tinklų ir informacinių sistemų (TIS) turtas – tai visi skaitmeniniai ar fiziniai IT duomenys, informacija ir žinios, turinčios vertę organizacijai, kurie naudojami veiklai vykdyti ir sprendimams priimti. Tai gali būti tiek duomenų bazės, intelektinė nuosavybė, dokumentai, programinė įranga, elektroninės komunikacijos ir kiti organizacijos naudojami informacijos šaltiniai, kurių praradimas ar neteisėta prieiga prie jų gali turėti neigiamų pasekmių.

Tinklų ir informacinės sistemos (TIS) – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais.

Turto savininkas (-ai) – turto savininkas yra asmuo ar padalinys, kuris yra atsakingas už konkrečius turto vienetus ir / ar grupes. Jie žino šiuos turto vienetus ar grupes ir rizikos valdymo proceso metu teikia žinias už rizikos valdymą atsakingam asmeniui.

5. Priedai

5.1–5.11 priedai

5.1–5.11 priedai pateikiami atskirai rizikos registre.

6. Šaltiniai

[1] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl aukšto bendro kibernetinio saugumo lygio visoje Sąjungoje (NIS2 direktyva), *https://eur-lex.europa.eu/eli/dir/2022/2555/oj*.

[2] Kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas (2024 m. liepos 11 d. Nr. XIV-2902), *https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/1a8657f2427a11efb121d2fe3a0eff27?j*.

[3] *https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee*.

[4] Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (Kibernetinio saugumo reikalavimų aprašas), *https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr*.