

Nr.	Kibernetinės saugos principai	Perteikimas (e-mokymų elementas)	Trukmė, min
	<p>Ugdoma kompetencija – Skaitmeninė.</p> <p>Tikslas – suteikti dalyviams išsamų supratimą apie kibernetinio saugumo principus, metodus ir praktikas, kurios padeda vertinti, valdyti ir reaguoti į kibernetines grėsmes organizacijoje.</p>		150
	Įžanga	Video	
	<p>Kibernetinis saugumas – tai veiksmai, kurių imamasi norint apsaugoti kibernetinę aplinką ir užtikrinti informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumą, vientisumą bei konfidencialumą.</p>	Statement	
	<p>4 iš 10 Lietuvos įmonių kibernetinio saugumo dar nelaiko prioritetine sritimi, rodo 2024 m. balandžio–gegužės mėnesiais „Luminor“ užsakymu tyrimų bendrovės „Norstat“ atlikta Baltijos šalių smulkaus ir vidutinio verslo vadovų apklausa.</p> <p>Šaltinis: https://data.kurkl.lt/wp-content/uploads/2023/04/SVV-kibernetinio-saugumo-apklauso-apzvalga-Kurk-Lietuvai.pdf).</p> <p>Kitas papildomas resursas - „Kurk Lietuvai“ projekto Krašto apsaugos ministerijoje vykdyta apklausa, siekiant įvertinti smulkiojo ir vidutinių verslo (SVV) įmonių kibernetinio saugumo sąmoningumą ir problematiką. SVV vadovų ir darbuotojų apklausa vykdyta „e.pilietis“ platformoje 2019 m. lapkričio – gruodžio mėnesiais. Bendras apklausose dalyvavusių respondentų skaičius – 227. Beveik trečdalis (32 %) SVV įmonių neturi darbuotojo, skyriaus ar išorinio paslaugų tiekėjo, kuris rūpintųsi įmonės kibernetiniu saugumu.</p> <p>Šaltinis: https://luminor.lt/lt/naujienos/tyrimas-lietuvos-verslas-savo-kibernetiniu-saugumu-rupinasi-maziausiai-is-baltijos-saliu).</p> <p>Siekiant įvertinti organizacijų kibernetinio atsparumo lygį, NKSC (Nacionalinio kibernetinio saugumo centras) periodiškai vertina organizacijų ir techninių priemonių taikymą ypatingos svarbos informacinę infrastruktūrą (toliau – YSII) valdančiose organizacijose.</p> <p>Organizacijų reikalavimų (pavyzdžiui, patvirtinta kibernetinio saugumo politika, ją įgyvendinantys standartai, procedūros ir kt.) įgyvendinimas YSII 2023 m. augo 10 proc., palyginti su 2022 m. duomenimis. Daugiau finansinių, žmogiškųjų resursų ir kompetencijų reikalaujančių techninių saugumo priemonių įgyvendinimas šiose organizacijose 2023 m. padidėjo 7 proc. [galima būtų įterpti grafiką ar vizualiai atvaizduoti pokytį/skaičius]</p>	Video	

NKSC skatina visas organizacijas, net tik YSII, savanoriškai savo veikloje taikyti organizacines ir technines kibernetinio saugumo priemones, nes jos gerokai mažina riziką patirti kibernetines atakas, užtikrina organizacijos veiklos tęstinumą ir mažina kibernetinių incidentų sukeltą žalą.

[pateikti informaciją kortelės pavidalu **YSII** – tai ryšių informacinė sistema ar jos dalis, ryšių informacinės sistemos grupė, kurioje įvykęs kibernetinis incidentas gali padaryti didelį neigiamą poveikį nacionaliniam saugumui, valstybės ūkiui, valstybės ir visuomenės interesams.]

Nuolatinis kibernetinių kompetencijų ugdymas yra viena iš svarbiausių valstybės atsparumo kibernetinėms grėsmėms didinimo priemonių

Kibernetinių atakų atvejai Lietuvoje

- Citybee (2021 m. vasaris)

Prarasta: 110 tūkstančių vartotojų duomenų.

2021 m. pradžioje internetiniame forume pasirodė „CityBee“ klientų duomenys. Piktavaliai paviešino vartotojų vardus ir pavardes, asmens kodus, telefonų numerius, elektroninio pašto adresus, gyvenamosios vietos adresus, mokėjimo kortelės detales, vairuotojų pažymėjimo numerius bei užšifruotus slaptažodžius.

- KTU (2023 m. gruodis)

Piktavaliai galėjo gauti nesankcionuotą prieigą prie šių Universiteto darbuotojų duomenų: vardo, pavardės, asmens kodo, gyvenamosios vietos adreso, telefono numerio, elektroninio pašto adreso, asmeninio automobilio valstybinių numerių. Buvo aptikta informacija, kad už vieną tokių duomenų paketą tamsiajame internete (angl. dark net) prašoma apytiksliai 315 tūkst. eurų.

- Vilniaus rajono savivaldybė (2023 m. gruodis)

Piktavaliai prašė šimtų tūkstančių dolerių vertės išpirkos. Savivaldybė tikina, jog svarstymų ją sumokėti nebuvo. Dėl šios patirtos kibernetinės atakos sutriko socialinių išmokų mokėjimas.

2023 m. suvestinė pagal dažniausiai aptiktus slaptažodžius naudojamus Lietuvoje

Nr	Slaptažodis	Slaptažodžio atspėjimo laikas	Kiekis
----	-------------	-------------------------------	--------

1	admin	< 1 Sekundė	2,720
2	123456789	< 1 Sekundė	1,454
3	123456	< 1 Sekundė	1,287
4	lopas123	17 Minučių	1,118
5	a1b9c1d9	3 Valandos	699
6	12345678	< 1 Sekundė	599
7	543212	1 Sekundė	555
8	vytautas	3 Valandos	538
9	nojukas123	1 Diena	533
10	jolanta333	1 Diena	501

[šaltinis - <https://nordpass.com/most-common-passwords-list/>]

Svarbu žinoti, kad kibernetinis saugumą užtikrinti padeda trys pagrindiniai aspektai:

- **Konfidencialumas**

Svarbu užtikrinti, kad bet kokia įmonės, klientų ar verslo partnerių informacija yra pasiekama tik įgaliotiems asmenims, kuriems būtina žinoti, ir jiems suteikta tokia prieiga. Konfidencialios informacijos pavyzdžiai: banko sąskaitų išrašai, darbuotojų ir klientų asmeninė informacija ar komercinės / gamybos paslaptys.

- **Vientisumas**

	<p>Svarbu užtikrinti, kad informacija ir duomenys yra teisingi - nėra atsitiktinai ar neteisėtai pakeisti ir sunaikinti. Duomenys dažniausiai suklaidojami dėl pakenkimo programinei įrangai ar neteisėto jos užvaldymo, techninės ar programinės įrangos gedimo.</p> <ul style="list-style-type: none"> ● Prieinamumas <p>Svarbu užtikrinti, kad visada būtų prieiga prie tam tikros informacijos, duomenų bazės ar kitų elektroninių paslaugų. Įmonėje tai galėtų būti nuolatinės svetainės ar duomenų bazės prieigos užtikrinimas. Sutrikus veiklai ir neturint galimybės pasiekti reikiamą informaciją, net ir trumpą laiką, įmonė gali būti priversta laikinai nutraukti savo veiklą ir prarasti pajamas, sukelti klientų nepasitenkinimą bei pakenkti savo reputacijai.</p> <p>Kibernetiniai incidentai gali grėsti visur, o bandymų įsilaužti į įmonių tinklus ar darbuotojų paskyras skaičius tik didėja, ir mažai tikėtina, kad ši tendencija artimiausiu metu keisis. Būtina suvokti, kad kibernetinės atakos auka gali tapti kiekviena organizacija, nepriklausomai nuo dydžio, vykdomos veiklos ar naudojamų kibernetinio saugumo priemonių modernumo.</p>		
1.	Organizacijos kibernetinio saugumo būklės vertinimas		
	<p>Viena iš daugelių organizacijos vadovo funkcija – užtikrinti, kad organizacija laikytųsi Lietuvos reglamentavimo reikalavimų. Vadovas turi nuolat susipažinti su teisės aktais, reglamentuojančiais kibernetinį saugumą, asmens duomenų apsaugą, informacijos saugumą ir kitais aktualiais reguliavimo aspektais. Visa informacija apie aktualius reglamentavimus ir naujienas šioje srityje gali būti randama Nacionalinio kibernetinio saugumo centro (NKSC) svetainėje - https://www.nksc.lt/aktualu.html</p>	Paragraph	
	<p>Teisinė atsakomybė</p> <p>Lietuvos Respublikos kibernetinio saugumo įstatymas apibrėžia, kad viešojo administravimo subjektai atsako už jų valdomų ir (arba) tvarkomų valstybės informacinių išteklių, o ypatingos svarbos informacinės infrastruktūros valdytojai – už jų valdomos ypatingos svarbos informacinės infrastruktūros kibernetinį saugumą.</p> <p>Lietuvos Respublikos kibernetinio saugumo įstatymas nustato kibernetinio saugumo principus ir procedūras, siekiant apsaugoti šalies informacines sistemas ir infrastruktūrą. Įstatymas reglamentuoja, kaip institucijos ir įmonės turi</p>	Video	

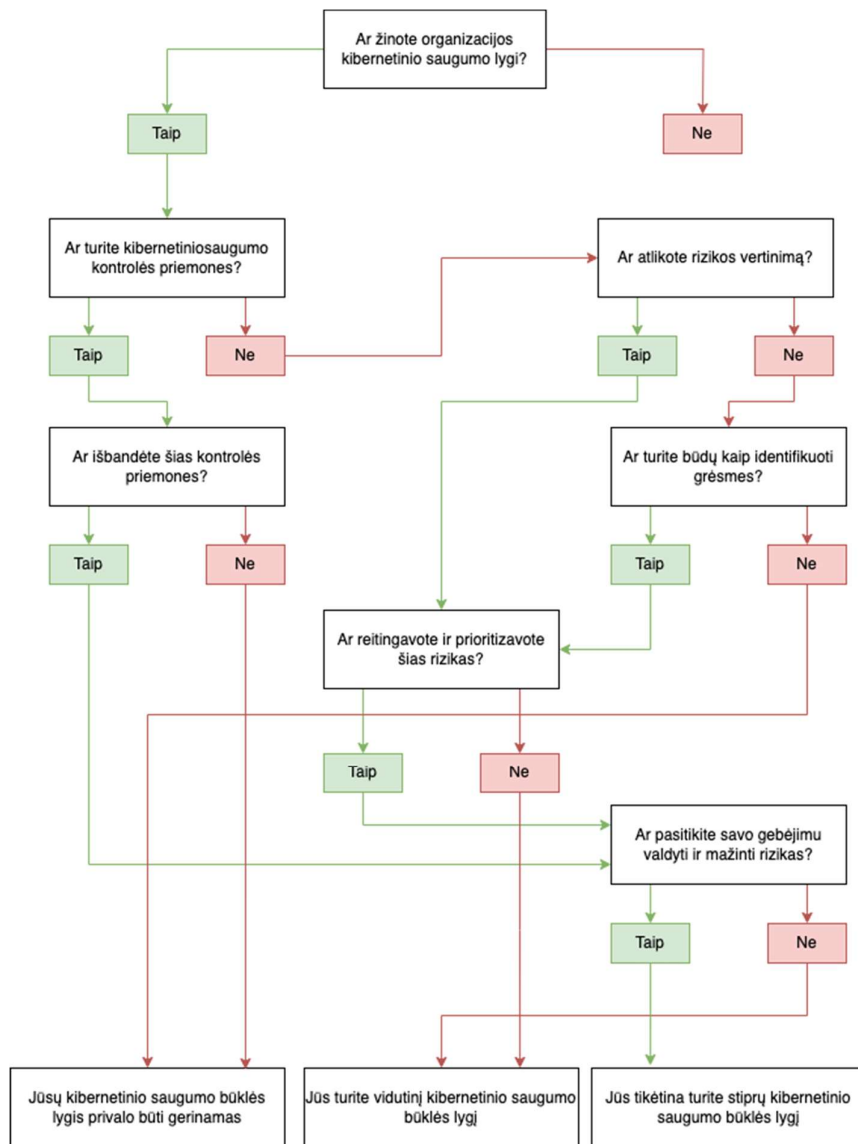
<p>elgtis kibernetinių grėsmių atveju, nustato jų pareigas bei atsakomybes. Be to, įstatymas apibrėžia kritinės infrastruktūros objektų sąrašą, kurie yra ypač svarbūs užtikrinant nacionalinį saugumą ir kuriems taikomi griežtesni saugumo reikalavimai. Taip pat įstatyme numatytos taisyklės dėl informacijos keitimosi tarp įvairių valstybės institucijų bei privačiojo sektoriaus subjektų, siekiant efektyviau valdyti ir atsakyti į kibernetinius incidentus.</p> <p>Kibernetinio saugumo įstatymas taikomas įvairioms institucijoms ir organizacijoms, kurios yra įtrauktos į šalies kibernetinio saugumo infrastruktūrą. Įstatymas reglamentuoja viešojo administravimo subjektų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir paslaugų teikėjų pareigas ir atsakomybes. Tai apima ir krašto apsaugos, vidaus reikalų bei kitas ministerijas, taip pat Nacionalinį kibernetinio saugumo centrą, kurie visi turi įgyvendinti tam tikras saugumo priemones ir procedūras, siekiant užtikrinti nacionalinį saugumą kibernetinėje erdvėje.</p> <p>(šaltinis https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/ITpnlvtcfz)</p>		
<p>BDAR (angl. GDPR) - Bendrasis duomenų apsaugos reglamentas</p> <p>BDAR nustato asmens duomenų tvarkymo, saugumo užtikrinimo reikalavimus, asmens duomenis tvarkančių (ar valdančių) subjektų teises ir pareigas bei duomenų subjektų – fizinių asmenų, kurių duomenys tvarkomi, teises.</p> <p>Reglamentas taikomas visiems ūkio subjektams, tvarkantiems (ar valdantiems) asmens duomenis.</p> <p>Duomenų apsaugos principų laikymasis ir atskaitomybė:</p> <ul style="list-style-type: none"> Užtikrinti, kad duomenų tvarkymas atitiktų BDAR principus: teisėtumą, sąžiningumą, skaidrumą, tikslų apribojimą, duomenų kiekio mažinimą, tikslumą, saugojimo trukmės apribojimą ir saugumą. Dokumentuoti ir įrodyti šių principų laikymąsi. <p>Organizacinių ir techninių saugumo priemonių įgyvendinimas:</p> <ul style="list-style-type: none"> Įdiegti tinkamas saugumo priemones, apsaugančias asmens duomenis nuo neteisėto tvarkymo, praradimo, sunaikinimo ar sugadinimo. Reguliariai peržiūrėti ir atnaujinti saugumo priemones, prisitaikant prie naujų grėsmių. <p>Duomenų subjektų teisių užtikrinimas:</p>	<p>Paragraph + Timeline / Accordeon</p>	

	<ul style="list-style-type: none"> • Informuoti duomenų subjektus apie jų teises ir užtikrinti jų įgyvendinimą, įskaitant teisę susipažinti su duomenimis, teisę ištaisyti, teisę ištrinti, teisę apriboti tvarkymą, teisę į duomenų perkeliamumą ir teisę prieštarauti duomenų tvarkymui. <p>Duomenų tvarkymo rizikos valdymas ir pažeidimų pranešimas:</p> <ul style="list-style-type: none"> • Atlikti rizikos vertinimus ir poveikio duomenų apsaugai vertinimus (DPIA) didelės rizikos atvejais. Dokumentuoti duomenų saugumo pažeidimus ir pranešti apie juos priežiūros institucijai per 72 valandas, jei pažeidimas kelia riziką asmenų teisėms ir laisvėms. <p>Duomenų tvarkytojų kontrolė ir duomenų apsaugos pareigūno paskyrimas:</p> <ul style="list-style-type: none"> • Užtikrinti, kad duomenų tvarkytojai laikytųsi BDAR reikalavimų per rašytines sutartis. Kai būtina, paskirti duomenų apsaugos pareigūną, atsakingą už BDAR laikymąsi organizacijoje, darbuotojų mokymą ir sąveiką su priežiūros institucijomis. <p>[https://vdai.lrv.lt/lt/naujienos/pokyciai-lietuvos-respublikos-asmens-duomenu-teisines-apsaugos-istatyme/]</p> <p>[https://vdai.lrv.lt/uploads/vdai/documents/files/el_ASMENS%20DUOMEN%C5%B2%20APSAUGA%20DARBO%20ANTYKI%C5%B2%20KONTEKSTE%20Gair%C4%97s%20smulkiajam%20ir%20vidutiniam%20verslui.pdf]</p> <p>[https://vdai.lrv.lt/uploads/vdai/documents/files/01_%20SolPriPa%20Asmens%20duomenu%20apsaugos%20gaire%20SMULKIAJAM%20IR%20VIDUTINIAM%20VERSLUI%202019-11-08.pdf]</p>		
	<p>TIS2 (angl. NIS2) - Tinklų ir Informacinių Sistemų Saugumo direktyvą</p> <p>2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva).</p> <p>[https://eur-lex.europa.eu/eli/dir/2022/2555/oj]</p>	Paragraph + Image & Text	

	<p>TIS 2 direktyva siekiama padidinti organizacijų, kurios įvairiuose sektoriuose atlieka itin svarbias funkcijas, kibernetinio atsparumo lygį, taip pat sumažinti kibernetinio atsparumo neatitikimus tarp sektorių ir sektoriuose bei pagerinti informacijos mainus ir kolektyvinius gebėjimus pasirėngti incidentams ir į juos reaguoti. Viešojo ir privataus sektoriaus laukia dideli pokyčiai, susiję su esminių ir svarbių subjektų identifikavimu, kibernetinio saugumo rizikų valdymo priemonių įgyvendinimu, kibernetinių incidentų valdymu bei kibernetinio saugumo subjektams taikoma priežiūra.</p>		
	<p>TIS 2 direktyvą įgyvendinančius teisės aktus planuojama priimti iki 2024 m. spalio 17 d. Už TIS 2 direktyvos 21 ir 23 straipsnių pažeidimą numatytos šios administracinės baudos:</p> <ul style="list-style-type: none"> • esminiems subjektams: iki 10 mln. Eur arba ne mažiau kaip 2 proc. bendros pasaulinės metinės apyvartos praėjusiais finansiniais metais, atsižvelgiant į tai, kuri suma didesnė; • svarbiems subjektams: iki 7 mln. Eur arba bent 1,4 % bendros pasaulinės metinės apyvartos praėjusiais finansiniais metais, atsižvelgiant į tai, kuri suma didesnė. <p>[https://kam.lt/tinklu-ir-informaciniu-sistemu-direktyva/]</p>	List	
1.1.	Kibernetinio saugumo būklės supratimas		
	<p>Organizacijos kibernetinio saugumo būklė atspindi bendrą jos tinklą, sistemų ir procedūrų saugumo būklę. Tai yra holistinis požiūris į bendras kibernetinio saugumo stiprumo ir atsparumo aspektus. Kibernetinio saugumo būklė gali būti išreikšta kaip matavimo vienetas, kuris įvertina Jūsų pasirėngimą gintis nuo kibernetinių grėsmių ir reaguoti į jas. Taip pat tai apima ir organizacijos saugumo mechanizmų, politikos ir procedūrų bendrą būklę. Suprasti ir gerinti savo kibernetinio saugumo būklę yra svarbu, norint apsaugoti savo turimą turtą (tiek fizinį, tiek skaitmeninį), išlaikyti verslo reputaciją ir kurti klientų pasitikėjimą.</p> <p>Norint geriau suprasti kibernetinio saugumo būklę, ją galima suskaidyti į sekančius elementus:</p> <p>Politikos ir procedūros:</p> <p>Tvirta kibernetinio saugumo būklė prasideda nuo gerai apibrėžtų saugumo politikų ir procedūrų. Šie dokumentai turėtų apibrėžti organizacijos požiūrį į kibernetinį saugumą. Tai gali apimti tokius dalykus kaip: incidentų reagavimo planai, duomenų apsaugos planai, kibernetinio saugumo mokymo planai ir pan. Planuose turėtų būti apimti ne vien</p>	Video + Tabs	

<p>tik IT (angl. Information Technology) dalį, bet ir OT (angl. Operational Technology) dalį. Šiuolaikinės technologijos vis labiau persidengia, todėl IT bei OT sistemų integracija yra neišvengiama. Politikos, kurios apima abi sritis, užtikrina, kad šios technologijos galėtų veikti kartu sklandžiai ir saugiai. Taip pat nereikėtų pamiršti ir atitikties procedūrų, kurios padeda bei užtikrina, kad organizacijoje būtų laikomasi teisinių, reguliavimo ir organizacinių reikalavimų, formuojančių veiksmingą kibernetinio saugumo būklės pagrindą.</p> <p>Techninės kontrolės: Techninės kontrolės arba techniniai sprendimai yra būtini apsaugai nuo kibernetinių grėsmių. Tai gali apimti ugniasienes ir įsilaužimų aptikimo sistemas (IDS), kurios stebi ir kontroliuoja tinklo srautą, šifravimo metodus, apsaugo duomenų konfidencialumą tiek ilsėjimosi “at-rest” metu, tiek perduodant duomenis, ir prieigos kontrolės mechanizmus, kurie užtikrina, kad tik įgaliojoti vartotojai galėtų pasiekti atitinkamą informaciją.</p> <p>Fizinis saugumas: Prieigos kontrolės sistemos ir stebėjimas, yra būtini, kad būtų išvengta neteisėtos fizinės prieigos prie kritinės ar svarbios infrastruktūros ar jos elementų. Šios priemonės papildo techninės kontrolės priemones, apsaugodamos organizacijos fizinius išteklius.</p> <p>Žmogiškieji veiksniai: Viso personalo kibernetinio saugumo gebėjimai yra labai svarbūs, ne tik IT. Kibernetinių gebėjimų bei raštingumo ugdymas turėtų būti vykdomas pastoviai (visais organizacijos lygmenimis), nes silpniausia grandis, deja, yra neišprusę vartotojai. Taip pat svarbu atkreipti dėmesį, jog aukšto lygio kibernetinių specialistų trūkumas gilina šią probleminę sritį. Žmogiškieji ištekliai gali atlikti svarbų vaidmenį palaikant stiprią kibernetinio saugumo būklę. Be to, organizacija, turėdama specialią incidentų reagavimo komandą, yra pasirengusi efektyviau valdyti ir sušvelninti kibernetinio saugumo incidentus.</p> <p>Stebėjimas ir aptikimas: Nuolatinis stebėjimas ir aptikimas yra ne mažiau svarbūs kibernetinio saugumo būklės komponentai. Saugumo informacijos ir įvykių valdymo (SIEM) įrankiai gali generuoti realaus laiko kibernetinio saugumo įspėjimus, leidžiančius organizacijai greitai aptikti ir reaguoti į esamas ar, galbūt, numatomas grėsmes. Taip pat verta atkreipti dėmesį, kad NKSC teikia pažeidžiamumų patikros paslaugą pagal užsakymą kibernetinio saugumo subjektams, kurie siekia įsivertinti savo sistemų saugumo būklę, bet neturi tam tinkamų įrankių ar lėšų tokio pobūdžio paslaugai įsigyti. Daugiau apie paslaugą ir jos užskaymas gali būti atlikas https://www.nksc.lt/paslaugos/pazeidziamumu-patikrinimas.html</p>		
--	--	--

	<p>Incidentų reagavimas ir atkūrimas:</p> <p>Incidentų reagavimo planas yra iš anksto aprašyta ir sutarta strategija, skirta valdyti ir sušvelninti kibernetinio saugumo incidento pasekmes. Taip pat organizacijos nelaimės padarinių likvidavimo (DRP) bei verslo tęstinumo (BCP) planų apjungimas, leistų dar efektyviau užtikrinti, kad kritinės sistemos bei duomenys būtų greitai atkurti po kibernetinio incidento ar kitos nelaimės.</p> <p>Kibernetinio Saugumo būklė vs kibernetinio saugumo atitiktis</p> <p>Kibernetinio saugumo būklė ir kibernetinio saugumo atitiktis gali ir privalo veikti kartu, tačiau tai nėra vienas ir tas pats dalykas. Saugumo atitiktis išreiškia priemones, kurias organizacija įgyvendina, kad atitiktų sutartinius arba reguliacinius reikalavimus. Kibernetinio saugumo būklė apima kibernetinės apsaugos priemones ar sprendimus, kurias organizacija taiko, siekdama apsaugoti savo IT turtą, duomenis ir klientus. Galima teigti, kad saugumo atitiktis labiau susijusi su taisyklių laikymusi, nustatytais specifiniais saugumo standartais ir reglamentais, o saugumo būklė - organizacijos gebėjimas apsisaugoti nuo išorinių grėsmių.</p>		
1.2.	Priemonės kibernetinio saugumo būklei vertinti		
	Šioje temoje pristatysime 10 žingsnių sistemą, kuri padėtų įvertinti kibernetinio saugumo būklę organizacijoje.	Video / Timeline + Image	



[Iliustracija - Supaprastintas kibernetinio saugumo būklės lygio nustatymas]

1) IT inventORIZACIJA

- Identifikuokite ir dokumentuokite turimus IT resursus, įskaitant aparatinę ar programinę įrangą ir duomenis.
- Įvertinkite kiekvieno išteklių prieigos teises ir jų būtinybę, būtina pabrėžti ir atkreipti dėmesį į trečiųjų šalių prieigą.
- Įsivertinkite skirtingų kibernetinių grėsmių tikimybę ir poveikį.

2) Rizikų prioretizavimas

- Naudokite rizikos analizės matricą, kuri skirta įvertinti bei reitinguoti rizikas pagal tikimybę ir poveikį.
- Atraskite organizacijoje resursų, kurie bus skirti spręsti aukšto lygio rizikas.
- Paruoškite veiksmų planą (-us), kurie atlieptų identifikuotas svarbiausias grėsmes.

3) Darbuotojų mokymai

- Įgyvendinkite kibernetinio saugumo mokymų testinę programą ar planą. Mokymai turėtų vykti tiek įdarbinimo metu, tiek sudarant galimybę žinias pastoviai atnaujinti ar tobulinti kada tam yra poreikis.
- Naudokite interaktyvius metodus pvz. praktinės ar teorinės kibernetinių incidentų simuliacijos, interaktyvios mokymų platformos, grupiniai gyvi mokymai ir pan. tam, kad sustiprintumėte mokymosi procesą bei žinias.

4) Kibernetinių incidentų valdymo planas

- Turėkite parengtus išsamius planus rizikoms valdyti.
- Priskirkite ir aprašykite aiškias roles ir atsakomybes incidentų reagavimo komandoje arba paskirkite darbuotojus, kurie galėtų prisiimti atitinkamas roles bei atsakomybes.
- Išsamiai dokumentuokite kibernetinius incidentus bei reguliariai peržiūrėkite ar numatytas veiksmų planas po incidento yra efektyviai įgyvendinamas.

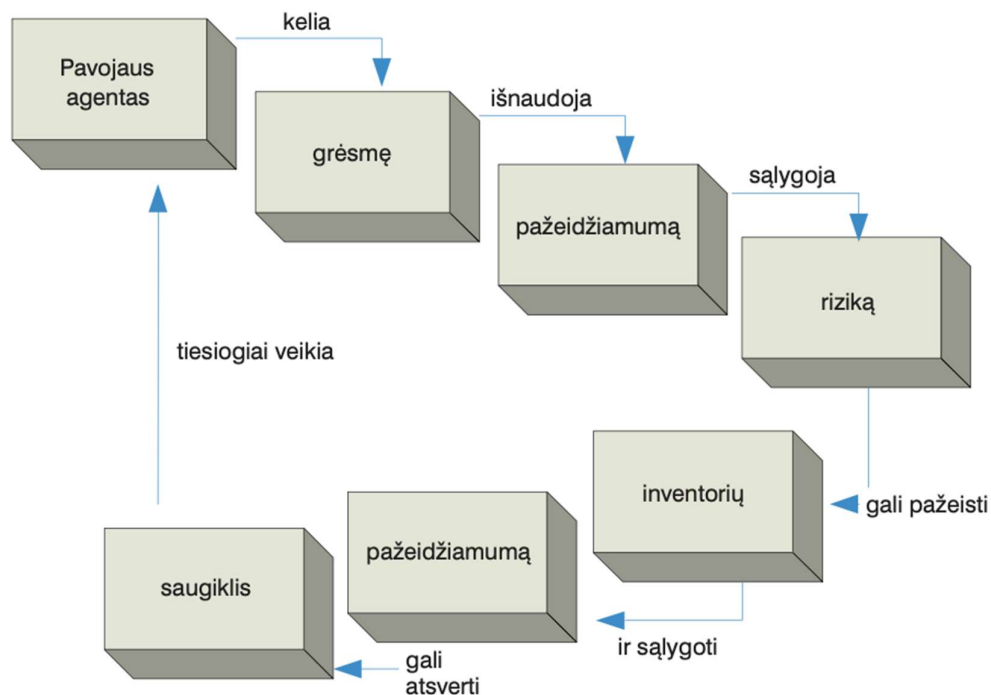
5) Kibernetinio saugumo metrikos

- Nusistatykite bent keletą elementarių metrikų /rodiklių, kurios privalo būti pastoviai stebimos pvz.: bandymų įsilaužti į sistemas kiekis, nustatytų pažeidžiamumų skaičius, kiek laiko trunka sutvarkyti nustatytus pažeidžiamumus, darbuotojų mokymų rodikliai ir t.t.
- Sekant išsikeltas metrikas / Stebėdami nustatytus rodiklius, nuolat vertinkite jų pokyčius bei atitinkamai koreguokite kibernetinio saugumo būklę ir su ja susijusius elementus.

	<p>6) Procesų automatizacija</p> <ul style="list-style-type: none"> • Automatizuokite pasikartojančių darbų procesus, pvz.: IT inventorizacijos bei nuolatinių pažeidžiamumų skenavimą, bazinius kibernetinio saugumo testavimus ir pan. • Naudokite techninius įrankius ar sprendimus, kurie turi galimybę apdoroti bei sujungti duomenis iš įvairių kibernetinio saugumo įrankių ar sistemų geresniam kibernetinio saugumo būklės matomumui. • Leiskite komandoms susitelkti į strategines kibernetinio saugumo būklės gerinimo iniciatyvas. <p>7) Nuolatinis testavimas ir stebėjimas kibernetinio saugumo kontrolės priemonių</p> <ul style="list-style-type: none"> • Reguliariai vykdykite kibernetinio saugumo ir vidinius auditų testus, siekiant nustatyti silpnąsias organizacijos vietas. • Įgyvendinkite nuolatinį IT sistemų stebėjimą, kad galėtumėte greitai aptikti ir reaguoti į kylančias grėsmes. • Reguliariai atnaujinkite ir įdiekite įvairius pakeitimus į turimas sistemas, kad išvengtumėte bandymų įsilaužti bei mažinti programinės įrangos pažeidžiamumų kiekį. <p>8) Kibernetinio saugumo ir atitikties automatizavimas</p> <ul style="list-style-type: none"> • Naudokite automatizavimo platformas rizikoms vertinti, trečiųjų šalių tiekėjų valdymui bei centralizuotu būdu stebėti organizacijos kibernetinio saugumo būklę. • Automatizuokite procesus, kurie padeda efektyviau rinkti įrodymus skirtus pateikti atitikties ar standartų vertinimo metu. Taip pat automatizuoti ataskaitų teikimą ir generavimą. <p>9) Vykdykite trečiųjų šalių teikiamas pažeidžiamumų vertinimų paslaugas ir įsibrovimo testavimą</p> <ul style="list-style-type: none"> • Samdykite išorinius ekspertus ar įmones, kurios geba atlikti įsibrovimų testavimą ir kibernetinio saugumo spragų analizę. • Reguliariai atnaujinkite vertinimo metodologijas ir kriterijus tam, kad būtų tinkamai atlieptos naujai kylančios kibernetinės grėsmės. <p>10) Užtikrinkite bei gerinkite atitiktį kibernetinio saugumo karkasams / sistemoms (angl. „Frameworks“)</p> <ul style="list-style-type: none"> • Laikykitės tokių karkasinių gairių / Vadovaukitės pagrindinėmis gairėmis kaip NIST, ISO/IEC 27001 ar Top 18 CIS Controls. • Reguliariai peržiūrėkite atitikties reikalavimus ir atnaujinkite organizacijoje taikomas kibernetinio saugumo priemones. 		
--	---	--	--

	<ul style="list-style-type: none"> Naudokite atitiktus standartus ar karkasų gaires kaip vieną iš pagrindų, gerinančių ir vystančių kibernetinio saugumo būklę organizacijoje. 		
2.	Kibernetinio saugumo rizikų valdymas ir identifikavimas		
	<p>Sėkminga rizikos analizė priklauso nuo daugelio įvairių veiksnių t. y. aiškiai apibrėžta apimtis, galiojantys dokumentai, nešališkumas, rizikos analizės proceso brandumas, informacijos ir duomenų saugos užtikrinimo metodai bei organizavimas, rizikos analizėje dalyvaujančių darbuotojų kompetencija, patirtis ir jų vaidmuo organizacijoje. Rizikos analizė yra privalomas procesas kiekvienai organizacijai, siekiančiai valdomosios saugos. Tačiau saugos valdymo procesas turi būti nukreiptas į kritinius veiksnus, kurių nepaisymas gali padidinti nesėkmės tikimybę.</p> <p>[Šaltinis - https://www.nksc.lt/doc/rizikos_analize.pdf]</p>	Paragraph	
2.1.	Rizikos valdymo pagrindai		
	Rizikų valdymas - struktūrizuotas ir sistemingas požiūris į rizikos nustatymą, analizę ir jos valdymą. Tai procesas, kurio tikslas yra sumažinti neigiamą rizikos poveikį organizacijos tikslams. Rizikų analizė turi būti privalomas procesas kiekvienai organizacijai, kuri siekia ar nori valdyti savo saugą visomis prasmėmis.	Paragraph	
	<p>Pagrindiniai elementai yra:</p> <ul style="list-style-type: none"> Rizikos identifikavimas - potencialių rizikų nustatymas, kurios gali turėti įtakos tikslų pasiekimui. Rizikos vertinimas - nustatytų rizikų analizė, siekiant įvertinti jų poveikį ir tikimybę. Rizikos mažinimas - veiksmų plano kūrimas ir įgyvendinimas, siekiant sumažinti rizikos įtaką arba tikimybę. Rizikos stebėseną ir kontrolę - nuolatinis rizikos valdymo proceso peržiūrėjimas ir koregavimas pagal naujas sąlygas ir patirtį. 	Flashcard stack / Labeled graphic	
	<p>Rizikos identifikavimas ir vertinimas</p> <p>Rizikos identifikavimas ir vertinimas yra esminiai rizikos valdymo proceso etapai. Identifikavimas apima galimų grėsmių nustatymą ir jų šaltinių išaiškinimą. Vertinimas atliekamas per:</p> <ol style="list-style-type: none"> Kokybinę analizę, kurioje aprašomi rizikos veiksniai ir jų poveikis. 	List	

	2. Kiekybinę analizę, kurioje vertinami rizikos veiksniai skaitmeniniais rodikliais, pavyzdžiui, tikimybės ir poveikio vertinimas.		
	<p>Rizikos mažinimo strategijos</p> <p>Rizikos mažinimo strategijos apima įvairius būdus ir priemones, skirtus sumažinti rizikos tikimybę ar poveikį. Pagrindinės strategijos gali būti:</p> <ul style="list-style-type: none"> ● Rizikos vengimas: veiklos, kuri gali sukelti riziką, nutraukimas. ● Rizikos sumažinimas: priemonių taikymas siekiant sumažinti rizikos poveikį. ● Rizikos perkėlimas: rizikos perdavimas kitam subjektui, pvz., draudimui. ● Rizikos priėmimas: rizikos poveikio priėmimas su sąlyga, kad tai bus valdoma. 	Labeled graphic	
	<p>Rizikos valdymo sistemos</p> <p>Rizikos valdymo sistemos yra struktūrizuoti procesai ir metodikos, skirtos nuolatiniam rizikos valdymui, kurios apima:</p> <ul style="list-style-type: none"> ● Politikos ir procedūros: Formalūs dokumentai, apibrėžiantys rizikos valdymo procesą organizacijoje. ● Įrankiai ir technologijos: Programinė įranga ir metodikos, padedančios stebėti ir valdyti rizikas. ● Atsakomybės paskirstymas: Aiškus rizikos valdymo atsakomybių paskirstymas tarp darbuotojų ir vadovybės. <p>Šie principai ir metodai leidžia efektyviai valdyti riziką, siekiant minimizuoti neigiamą jos poveikį ir užtikrinti organizacijos tikslų pasiekimą.</p>	Process	
	<p>Rizikos analizės strategijos</p> <p>Atliekant rizikos analizę, būtina įvertinti rizikos grėsmės, pažeidžiamumo, vertybių, saugos valdymo priemonių ir tarpusavio sąsajos aspektus. Sekantis procesas iliustruoja saugos komponentų tarpusavio sąsajas, parodant, kaip įvairūs veiksniai sąveikauja tarpusavyje ir formuoja bendrą rizikos valdymo schemą.</p>	Paragraph	



[Iliustracija - Skirtingų saugos komponentų tarpusavio sąsajos].

- **Pavojaus agentas** – tai veiksnys ar objektas, kuris kelia grėsmę organizacijai. Tai gali būti įvairūs fiziniai, kibernetiniai ar aplinkos veiksniai.
- **Grėsmė** – pavojaus agentas kelia grėsmę, kuri gali išnaudoti organizacijos pažeidžiamumus. Grėsmės gali būti įvairios – nuo kibernetinių atakų iki gamtos stichijų.
- **Pažeidžiamumas (I)** – tai organizacijos silpnybės, kurias gali išnaudoti grėsmės. Pažeidžiamumai gali būti susiję su technologijomis, procedūromis, žmogiškaisiais veiksniais ar kitais aspektais.
- **Rizika** – pažeidžiamumas sąlygoja riziką. Rizika yra galimybė, kad grėsmė išnaudos pažeidžiamumą ir sukels neigiamas pasekmes.

Video + Image + Table

- **Inventorius** – tai organizacijos turtas, kuris gali būti paveiktas rizikos. Inventorius gali apimti tiek fizinį turtą, tiek informacinius išteklius.
- **Pažeidžiamumas (II)** – inventorius gali sąlygoti pažeidžiamumą, nes tam tikri turto elementai turi skirtingą pažeidžiamumo lygį, pvz.: serveris su operacine sistema, kuri nėra reguliariai atnaujinama yra labiau pažeidžiamas nei serveriai su operacine sistema, kuri yra reguliariai atnaujinama ir prižiūrima. Pažeidžiamumo įvertinimas yra būtinas siekiant suprasti, kaip apsaugoti svarbiausius išteklius.
- **Saugiklis** – tai apsaugos priemonės, kurios gali atsverti pažeidžiamumą. Saugikliai apima įvairias priemones ir strategijas, skirtas sumažinti grėsmių poveikį ir apsaugoti organizaciją.
- **Tiesioginis veikimas** – pavojaus agentas yra tiesiogiai veikiamas saugiklio, kuris savo ruožtu gali atsverti egzistuojantį pažeidžiamumą.

Efektyvi rizikos analizė reikalauja nuodugnaus kiekvieno šių veiksnių ir komponentų įvertinimo ir supratimo, siekiant užtikrinti organizacijos saugumą ir stabilumą.

Kita iliustracija - rizikos valdymo elementų tarpusavio santykiai, parodo, kaip atitinkami elementai sąveikauja tarpusavyje, sudarant kompleksinę rizikos valdymo schemą. Efektyvi rizikos analizė ir valdymas reikalauja suprasti šių elementų tarpusavio ryšius ir tinkamai valdyti grėsmes, pažeidžiamumus, riziką, inventorių ir saugos priemones, siekiant užtikrinti visapusišką organizacijos saugumą ir stabilumą. [ija - Rizikos valdymo elementų tarpusavio santykiai].

Elementas	Santykis
Grėsmės	<ul style="list-style-type: none"> ● Didina riziką - grėsmės tiesiogiai padidina organizacijos riziką, nes jos gali sukelti neigiamų pasekmių. ● Išnaudoja pažeidžiamumus - grėsmės gali pasinaudoti organizacijos silpnomis vietomis pvz.: pažeidžiamumais, kad sukeltų žalą.
Pažeidžiamumai	<ul style="list-style-type: none"> ● Didina riziką - pažeidžiamumai padidina riziką, nes jie sudaro sąlygas grėsmėms pakenkti. ● Kelia grėsmę inventoriui - pažeidžiamumai gali tiesiogiai kelti grėsmę organizacijos inventoriui, jei jie nėra tinkamai apsaugoti.
Inventorius	<ul style="list-style-type: none"> ● Turi vertę - inventorius turi vertę organizacijai, nes jis yra būtinas jos veiklai ir tikslų pasiekimui.

		<ul style="list-style-type: none"> Kelia grėsmę - jei inventorius yra pažeidžiamas, tai gali tapti grėsme, nes jo praradimas ar pažeidimas gali sukelti didelių nuostolių. 		
	Vertė	<ul style="list-style-type: none"> Didina riziką - kuo didesnė inventoriaus vertė, tuo didesnė rizika, nes jo praradimas, pažeidimas ar kitoks poveikis turi didesnes pasekmes organizacijai. 		
	Rizika	<ul style="list-style-type: none"> Didina vertę - rizika gali padidinti inventoriaus vertės suvokimą pvz.: kritinės informacinės sistemos ar kitas organizacijos veikslai užtikrinti inventorius. Tai reiškia, kad reikės imtis papildomų priemonių, norint apsaugoti vertingus išteklius. Didina saugos priemonių poreikį - aukštas rizikos lygis reikalauja daugiau saugos priemonių, siekiant sumažinti potencialius nuostolius. Kelia saugos reikalavimus - rizikos lygis daro įtaką saugos reikalavimams ir jų atitikimui, kurie gali nustatyti, kokių atitinkamų priemonių reikėtų imtis. 		
	Saugos reikalavimai	<ul style="list-style-type: none"> Reikalauja saugos priemonių - saugos reikalavimai apibrėžia, kokių saugos priemonių reikia imtis ir kaip jas reikėtų įgyvendinti siekiant sumažinti riziką. 		
	Saugos priemonės	<ul style="list-style-type: none"> Mažina riziką - saugos priemonės tiesiogiai mažina riziką, apsaugodamos organizaciją nuo galimų grėsmių ir pažeidžiamumų. Reikalauja saugos reikalavimų: Saugos priemonės turi atitikti tam tikrus reikalavimus, kurie būtų veiksmingi ir efektyvūs. Saugo nuo grėsmių - saugos priemonės tiesiogiai saugo organizaciją nuo identifikuotų arba potencialių grėsmių. 		
2.2.	Grėsmių modeliavimas ir analizė			
	Dažniausiai naudojamos grėsmių modeliavimo ir vertinimo sistemos 1. STRIDE Sukurta Microsoft, siekiant padėti nustatyti galimas saugumo grėsmes programinės įrangos kūrimo projektavimo etape. Jis sutelktas į grėsmių klasifikavimą pagal atakos tipą. STRIDE sistema naudoja grėsmių klasifikaciją pagal šešias kategorijas: Spoofing (Apgaulė), Tampering (Klaidinimas), Repudiation (Neigimas), Information Disclosure (Informacijos atskleidimas), Denial of Service (Paslaugos atsisakymas), Elevation of Privilege (Privilegijų suteikimas).		Carousel / Timeline / Video?	

	<p>Privalumai:</p> <ul style="list-style-type: none"> ● Pakankamai išsamus, struktūruotas bei apima platų grėsmių spektrą ir jų klasifikaciją. ● Plačiai naudojamas bei globaliai pripažintas. ● Labai gerai dokumentuotas. <p>Trūkumai:</p> <ul style="list-style-type: none"> ● Per daug orientuotas į technines grėsmes, neatsižvelgiant į verslo kontekstą. ● Ganėtinai sudėtingas pradedantiesiems. ● Reikalauja ganėtinai nemažai vidinių išteklių (laiko ir pastangų), norint jį pilnai įgyvendinti. <p>2. DREAD</p> <p>Taip pat sukurtas Microsoft. Jis naudojamas kiekybiškai įvertinti ir nustatyti prioritetinėms kibernetinio saugumo rizikoms, kurios atsiranda iš potencialių grėsmių. Tai padeda suprasti grėsmių poveikį ir jų tikimybę, taip pat kurioms grėsmėms reikėtų skirti didžiausią dėmesį.</p> <p>DREAD sistema naudoja grėsmių klasifikaciją pagal penkias kategorijas: Damage (Žalos dydis), Reproducibility (Atkuriamumas), Exploitability (Išnaudojimo galimybės), Affected Users (Nukentėję naudotojai) ir Discoverability (Atradimo galimybė).</p> <p>Privalumai:</p> <ul style="list-style-type: none"> ● Orientuotas į kiekybinį grėsmių aspektą, kuris padeda pagal svarbą identifikuoti grėsmes. ● Lengvai suprantamas bei įgyvendinamas. <p>Trūkumai:</p> <ul style="list-style-type: none"> ● Rizikos balų skyrimas (įprastai nuo 1 iki 10) gali skirtis priklausomai nuo asmeninių perspektyvų. ● Koncentruojasi tik į technines grėsmes, neatsižvelgiant į platesnį jų poveikį organizacijai pvz.: reputacijos žala. <p>3. PASTA</p> <p>PASTA (Process for Attack Simulation and Threat Analysis) yra septynių žingsnių metodika grėsmių nustatymui, analizavimui ir jų suskirstymui pagal svarbą. Metodas smarkiai akcentuoja tai, jog kibernetinės grėsmės būtų įžvelgiamos per rizikų prizmę.</p> <p>Privalumai:</p> <ul style="list-style-type: none"> ● Ganėtinai išsamus, nes reikalauja atlikti detalią analizę ir rizikos vertinimą. ● Lengvai pritaikomas konkrečioms organizacijos poreikiams. 		
--	---	--	--

	<ul style="list-style-type: none"> • Fokusuojasi į ankstyvą grėsmių nustatymą ir jų svarbos nustatymą. <p>Trūkumai:</p> <ul style="list-style-type: none"> • Ganėtinai sudėtingas ir patartina turėti ankstesnės patirties dirbant su šiuo metodu. • Imlus laiko prasme, nes metodas turi nemažai papildomų žingsnių, kuriuos reikėtų atlikti tam, kad tinkamai juo naudotis. <p>4. LINDDUN</p> <p>Skirtas duomenų privatumo pažeidžiamumams nustatyti. Jis buvo sukurtas siekiant padėti analizuoti ir užtikrinti asmens duomenų apsaugą informacinių sistemų kūrimo metu. LINDDUN sistema privatumo pažeidžiamumus klasifikuoja į septynias kategorijas: Linkability (Susiejamumas), Identifiability (Identifikuojamumas), Non-repudiation (Veiksmų nepripažinimo paneigimas), Detectability (Aptinkamumas), Disclosure of information (Informacijos atskleidimas), Unawareness (Nežinojimas) ir Non-compliance (Atitikties nesilaikymas).</p> <p>Ši sistema gali būti naudinga nustatant neatitikimus su ES 2016/679 BDAR reglamentu ir atitiktimi pagrindiniams šio reglamento nustatytiems "privatumo pagal dizainą" (angl. „privacy by design“) ir "privatumo pagal numatytąją nuostatą" (angl. „privacy by default“) principams. Svarbu paminėti, kad ši sistema labiau skirta suderinamumo analizei su privatumo reglamentais nei techninių pažeidžiamumų identifikavimui.</p> <p>Privalumai:</p> <ul style="list-style-type: none"> • Specifiškai skirtas privatumo apsaugai, leidžia identifikuoti ir spręsti grėsmes, kurios susijusios su privatumu. • Ganėtinai detalus ir išsamus, galima atlikti išsamią privatumo poveikio analizę. • Gali būti pritaikytas įvairioms informacinėms sistemoms ir organizacijoms, atsižvelgiant į specifinius poreikius. <p>Trūkumai:</p> <ul style="list-style-type: none"> • Galimai per siauras bendram saugumo grėsmių valdymui. • Reikalauja detalaus supratimo apie informacinių sistemų veikimą ir specifinių žinių apie privatumą ir duomenų apsaugą. • Reikalauja nemažai laiko, žmogiškųjų išteklių ir technologinių resursų. Tai gali būti sudėtinga mažesnėms organizacijoms su ribotais ištekliais. <p>5. OCTAVE</p>		
--	--	--	--

	<p>OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) sistema sukurta Carnegie Mellon universiteto Programinės įrangos inžinerijos instituto. Ši sistema padeda organizacijoms nustatyti, prioritetizuoti ir valdyti informacinio saugumo rizikas. OCTAVE pagrinde orientuojasi į rizikas, susijusias su organizacijos veikla, misija ir strategijos vertinimu, ne vien tik į techninius pažeidžiamumus.</p> <p>Privalumai:</p> <ul style="list-style-type: none"> ● Integruotas požiūris į organizacinius ir technologinius veiksnius. ● Apima įvairius kibernetinio saugumo aspektus, įskaitant strategines, operacines ir technines rizikas. ● Gali būti pritaikytas įvairaus dydžio ir tipo organizacijoms. ● Lanksti metodika, kurią galima pritaikyti pagal specifinius organizacijos poreikius. ● Į rizikos vertinimo procesą stengiamasi įtraukti įvairias suinteresuotąsias šalis organizacijos viduje, užtikrinant platų rizikų supratimą. ● Skatina kelti organizacijos sąmoningumo lygį bei kibernetinio saugumo rizikų valdymą. <p>Trūkumai:</p> <ul style="list-style-type: none"> ● Gali būti per sudėtingas ir ilgas procesas mažoms organizacijoms. ● Gali būti ne toks efektyvus greitai besikeičiančiose aplinkose. ● Reikalauja gana nemažai laiko, pastangų ir žmogiškųjų išteklių efektyviam įgyvendinimui. ● Gali būti sudėtinga mažesnėms organizacijoms su ribotais ištekliais. ● Gali būti netinkamas organizacijoms, kurioms reikia greito rizikos vertinimo. <p>Būtina atkreipti dėmesį, jog egzistuoja kelios išvestinės OCTAVE versijos t. y. OCTAVE Allegro ir OCTAVE-S.</p> <p>OCTAVE Allegro - orientuotas į įvairių dydžių organizacijas, dėmesys skiriamas efektyviam organizacijos turto rizikų identifikavimui ir mažinimui.</p> <p>OCTAVE-S - orientuotas į mažas ir vidutines organizacijas, dėmesys skiriamas kibernetinio saugumo rizikoms ir pažeidžiamumams.</p> <p>Kaip pasirinkti tinkama grėsmių modeliavimo ir vertinimo sistemą</p> <p>Vienareikšmiško atsakymo, kuri sistema tinkamiausia nėra - tai priklauso nuo organizacijos tikslų, norų ir strategijos.</p> <p>Jei privatumas yra svarbus (pvz., tvarkote jautrius asmens duomenis) įtraukite LINDDUN. Tačiau žvelgiant plačiau t. y. per platesnį organizacijos rizikų vertinimą, galimai tinkamesnė sistema būtų OCTAVE.</p>	
--	--	--

	<p>Jei pagrindinis tikslas yra prioretizuoti grėsmes pagal galimą jų poveikį tuomet DREAD sistema galėtų būti naudinga šiuo atveju. Jei tikslas yra identifikuoti saugumo grėsmes naujai kuriamose aplikacijose / sistemose - tinkamesnis būtų STRIDE. Verta paminėti, kad skirtingi modeliai gali būti naudojami skirtinguose organizacijos brandos etapuose ar vykdam tam tikrą veiklą, pavyzdžiui:</p> <ul style="list-style-type: none"> • Informacinių sistemų architektūros metu - STRIDE. • Bendram rizikų valdymui - OCTAVE arba PASTA. • Asmens duomenų apsauga ir asmens duomenys - LINDDUN. <p>Verta atsižvelgti ir į tai, kad organizacija gali naudoti kelias sistemas vienu metu. Tokia praktika yra dažnai sutinkama, kuomet organizacijos naudoja daugiau nei vieną sistemą tam, kad būtų apimti įvairūs ir skirtingi organizacijos aspektai. Pagrindinis aspektas yra tas, jog organizacija turėtų gerai įsivertinti savo specifinius kibernetinio saugumo poreikius, atsižvelgti į tvarkomus bei turimus duomenis, informacines sistemas ir bendrą IT ūkio kiekį. Kelių sistemų derinimas tarpusavyje gali suteikti išsamesnį ir platesnį požiūrį į kibernetinių grėsmių modeliavimą.</p>		
3.	Kibernetinių Incidentų reagavimas ir valdymas		
	<p>[Šaltinis - https://cris.mruni.eu/cris/entities/etd/a611e234-8754-4256-926c-fa5d7b551dc3] [Šaltinis - https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management] [Šaltinis - https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/cbddab726c5b11eea182def3ac5c11d6?positionInSearchResults=0&searchModeUUIID=b95cc445-ea54-4923-b05e-1c257bbbccbb]</p> <p>Kibernetinių incidentų reagavimas ir valdymas – tai procesai ir procedūros, skirtos aptikti, analizuoti ir reaguoti į kibernetinius incidentus, siekiant sumažinti jų poveikį ir užtikrinti organizacijos informacinių sistemų saugumą bei veiklos tęstinumą. Kibernetinis incidentas gali apimti įvairias grėsmes, tokias kaip kenkėjiškos programos, įsibrovimai, duomenų nutekėjimai ar kitokios kibernetinės atakos. Reagavimas į kibernetinius incidentus yra neatsiejamas nuo kibernetinio saugumo valdymo, kuris apima prevencijos, detektavimo, atsakymo ir atkūrimo veiklas.</p>	<p>Paragraph</p> <p>IV video</p>	
	<p>Lietuvos Respublikos krizių valdymo ir civilinės saugos įstatymo 11 straipsnio 5 dalis nurodo Vyriausybės atsakomybę užtikrinti operatyvų ir veiksmingą reagavimą į krizines situacijas. Ši nuostata gali būti tiesiogiai susijusi su kibernetinių incidentų reagavimu ir valdymu organizacijose keliais aspektais:</p>	IV video	

	<ul style="list-style-type: none"> • Koordinacija tarp institucijų - kibernetiniai incidentai dažnai reikalauja bendradarbiavimo tarp įvairių institucijų, įskaitant valstybės institucijas, IT departamentus, saugumo tarnybas ir teisėsaugą. Įstatymo 11 straipsnio 5 dalis akcentuoja koordinuotą veiksmų vykdymą, kuris yra būtinas efektyviam kibernetinių incidentų valdymui. • Krizių valdymo planų rengimas ir įgyvendinimas - organizacijos turi turėti parengtus kibernetinių incidentų valdymo planus, kurie būtų suderinti su nacionalinėmis saugumo strategijomis. Įstatymo 11 straipsnio 5 dalis reikalauja tokių planų, kurie apimtų ne tik fizinių, bet ir kibernetinių grėsmių valdymą. • Viešojo informavimo sistemų užtikrinimas - kibernetiniai incidentai gali turėti plačias pasekmes visai visuomenei, todėl yra svarbu užtikrinti veiksmingą komunikaciją su visuomene. Įstatymo 11 straipsnio 5 dalis pabrėžia viešojo informavimo svarbą, kas yra esminė dalis kibernetinių incidentų valdymo. • Operatyvus reagavimas - krizių valdymo ir civilinės saugos įstatymas pabrėžia operatyvaus reagavimo svarbą, kuris yra ypač aktualus kibernetinių incidentų metu. Greitas ir koordinuotas atsakas gali sumažinti incidento poveikį ir užkirsti kelią tolesnei žalai. 		
	Šių nuostatų įgyvendinimas reikalauja, kad organizacija turėtų aiškiai aprašytus kibernetinių incidentų valdymo procesus, kurie būtų suderinti su nacionalinėmis saugumo politikomis ir strategijomis. Tai apima technines priemones, žmogiškuosius resursus ir procedūras, skirtas greitam ir efektyviam reagavimui į kibernetinius incidentus.	IV video	
3.1.	Vidinių kibernetinių incidentų valdymas ir pasiruošimas		
	<p>Kibernetinių incidentų valdymas reikalauja sistemingo ir struktūruoto požiūrio. Pirmiausia, organizacijos turi sukurti (arba galbūt turi) aiškią kibernetinio saugumo politiką bei planus, kurie apimtų:</p> <ul style="list-style-type: none"> • Rizikų vertinimą ir valdymą - nustatant galimas grėsmes ir jų poveikį, sukurti rizikos mažinimo priemonių sąrašą. • Prevencines priemones - diegti tinkamas technines ir organizacines priemones, tokias kaip ugniasienės, antivirusinės programos, darbuotojų mokymai, kibernetinės saugos politikos ir kt. • Incidentų detektavimo sistemas - stebėti tinklą ir informacines sistemas, kad būtų galima laiku aptikti kibernetinius incidentus. 	IV video	

	<ul style="list-style-type: none"> Incidentų valdymo procesus - apibrėžti veiksmų planą incidento atveju, įskaitant atsakomybės paskirstymą ir informavimo procedūras. 		
	<p>Kibernetinių incidentų reagavimo planas Kibernetinių incidentų reagavimo planas yra dokumentas, kuriame apibrėžiamos veiksmų sekos ir atsakomybės reaguojant į kibernetinį incidentą. Šis planas turėtų apimti:</p> <ul style="list-style-type: none"> Incidentų klasifikaciją - nustatyti incidentų tipus ir jų rimtumą. Atsakomybės paskirstymas - aiškiai nurodyti, kas organizacijoje yra atsakingas už kiekvieną reagavimo etapą. Informavimo procedūra - apibrėžti, kaip ir kada informuoti suinteresuotąsias šalis (tiek vidines, tiek išorines) pvz.: vadovybę, darbuotojus, teisėsaugos institucijas ir kt. Atkūrimo veiksmus - nustatyti veiksmus, reikalingus informacinių sistemų ir paslaugų atkūrimui po incidento. 	Flashcards / Labeled graphic	
	<p>Vidinės kibernetinių incidentų komandos sukūrimas, vaidmuo ir atsakomybės Vidinės kibernetinių incidentų komandos (CIRT – Computer Incident Response Team) sukūrimas yra esminis žingsnis organizacijos kibernetiniam saugumui užtikrinti. CIRT komandos vaidmuo apima:</p> <ul style="list-style-type: none"> Incidentų stebėjimą ir analizę - nuolat stebėti informacines sistemas, aptikti ir analizuoti kibernetinius incidentus. Reagavimą į kibernetinius incidentus - sugebėti greitai ir efektyviai reaguoti į kibernetinius incidentus, siekiant sumažinti jų poveikį. Tyrimų atlikimą - vykdyti kibernetinių incidentų tyrimus, nustatyti jų atsiradimų priežastis ir sukurti rekomendacijas ateities prevencijai. Bendradarbiavimą - bendradarbiauti bei komunikuoti su kitomis organizacijos dalimis ir išorinėmis institucijomis, užtikrinant veiksmingą informacijos sklaidą. 	List	
	<p>Pagrindiniai kibernetinių incidentų reagavimo sistemos elementai</p> <p>Kibernetinių incidentų reagavimo sistema turi apimti šiuos pagrindinius elementus:</p>	Tabs	

	<ul style="list-style-type: none"> • Politikos ir procedūros - turi būti aiškiai apibrėžtos politikos ir procedūros, kurios nustatytų reagavimo į kibernetinius incidentus tvarką. • Techninės priemonės - naudoti pažangias ir naujausias technologijas, tokias kaip įsibrovimų detektavimo ir prevencijos sistemos (IDS/IPS), SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response) ar pan. sistemas. • Žmogiškieji ištekliai - turėti apmokytą specialistų komandą, kuri yra pasirengusi reaguoti į kibernetinius incidentus ir atlikti su jais susijusius tyrimus. • Mokymai ir pratybos: Nuolat mokyti darbuotojus ir atlikti praktines pratybas, siekiant užtikrinti jų pasirengimą. 		
	<p>Kibernetinių incidentų mokymai ir pratybos</p> <p>Kibernetinių incidentų mokymai ir pratybos yra būtini norint užtikrinti, kad visi organizacijos nariai reikalui esant būtų pasirengę reaguoti į vykstančius incidentus. Mokymų ir pratybų tikslai turėtų koncentruotis į:</p> <ul style="list-style-type: none"> • Sąmoningumo didinimą - informuoti darbuotojus apie galimas kibernetines grėsmes ir jų atpažinimo būdus. • Praktinius įgūdžius - suteikti darbuotojams praktinių įgūdžių, kurie padėtų efektyviai reaguoti į įvairius kibernetinius incidentus. • Testuoti planus - išbandyti incidentų reagavimo planus ir identifikuoti jų silpnąsias vietas. Tai gali būti atliekama atliekant realias atakas arba jas simuliuojant/imituojant (angl. „tabletop exercise“) • Bendradarbiavimo tobulinimas - Skatinti komandas ir kitų organizacijos dalių tarpusavio bendradarbiavimą incidentų metu. 	Accordeon	
3.2.	Kibernetinių incidentų komunikacija ir veikla po jų		
	<p>Efektyvi komunikacija kibernetinio incidento metu yra vienas iš esminių elementų, siekiant užtikrinti tinkamą reagavimą ir valdymą. Svarbu paminėti ir atkreipti dėmesį į sekančius aspektus:</p> <p>1. Komunikacijos plano parengimas</p> <ul style="list-style-type: none"> • Organizacija turėtų parengti detalų komunikacijos planą, kuris būtų įtrauktas į bendrą kibernetinių incidentų valdymo planą. Plane turėtų būti nurodyta, kas atsako už komunikaciją, kokie informavimo kanalai bus naudojami ir kokia informacija turi būti teikiama. • Sukurti krizės komunikacijos strategiją, kuri padėtų greitai ir efektyviai reaguoti į neplanuotas situacijas, tokiu būdu sumažinant galimą neigiamą poveikį organizacijos reputacijai. <p>2. Informacijos pateikimas:</p>	Timeline / Process	

	<ul style="list-style-type: none"> • Komunikacija turi būti aiški, tiksli ir pateikiama laiku. Būtina pabrėžti, kad informacija turėtų būti teikiama laiku. Reikėtų vengti perteklinės techninės informacijos, kadangi tai gali apsunkinti pačios informacijos supratimą ir jos esmę. • Suinteresuotosios šalys turi būti nuolat informuojamos apie incidento eigą, kokių priemonių buvo imtasi ir kokie buvo pasiekti rezultatai per laiko intervalą. Toks elgesys padeda išlaikyti pasitikėjimą suinteresuotų šalių ir užtikrina, kad visi susiję kibernetinio incidento dalyviai yra vienodai informuoti. <p>3. Vidinė ir išorinė komunikacija:</p> <ul style="list-style-type: none"> • Informuoti visus organizacijos narius apie kibernetinį incidentą, jo eigą ir kokių prevencinių priemonių buvo imtasi. Informavimo būdų ir metodų yra įvairių, svarbiausia išlaikyti ir naudoti tuos būdus, kurie yra paplitę organizacijoje pvz.: komunikacija, vykdoma per Microsoft Teams. Papildomai gali būti organizuojami visuotiniai ar komandiniai susirinkimai informacijos sklaidai. • Svarbu nepamiršti informuoti organizacijos klientus, partnerius ir teisėsaugos institucijas apie kibernetinį incidentą ir veiksmus, kurių buvo imtasi siekiant išspręsti ar suvaldyti situaciją. Tai gali būti spaudos pranešimai, socialinių tinklų panaudojimas, žiniasklaidos priemonės ar tiesioginis bendravimas su suinteresuotomis šalimis. 		
	<p>Kibernetinių incidentų pranešimas suinteresuotiems asmenims</p> <p>Kibernetinių incidentų pranešimai suinteresuotiems asmenims yra svarbus žingsnis siekiant užtikrinti sklandų informacijos perdavimą ir tinkamą reagavimą. Dažna praktika yra turėti jau paruoštus pranešimų šablonus su reikiama informacija tam, kad reikalui esant galima būtų greitai redaguoti tik reikiamas pranešimo vietas.</p>	Paragraph	
	<p>Galimi pranešimų tipai:</p> <ul style="list-style-type: none"> • Vidiniai pranešimai - tai pranešimai skirti organizacijos darbuotojams ir vadovybei. Jie turi būti trumpi, aiškūs ir informatyvūs, kad būtų galima greitai suprasti esamą situaciją ir imtis atitinkamų veiksmų, jeigu tai yra nurodyta. • Išoriniai pranešimai - tai pranešimai skirti klientams, partneriams, tiekėjams ar teisėsaugos institucijoms. Šie pranešimai turi pateikti esminę informaciją apie kibernetinį incidentą ir veiksmus, kurių buvo imtasi siekiant jį suvaldyti. 	Flashcards	

	<p>Galima pranešimo struktūra:</p> <ul style="list-style-type: none"> ● Incidento aprašymas - trumpai ir aiškiai aprašyti kas įvyko. ● Poveikio aprašymas - suteikti informaciją kokią įtaką incidentas turėjo ar potencialiai dar gali turėti organizacijos veiklai ir suinteresuotoms šalims. ● Imtasi veiksmai - išdėstyti ir paaiškinti kokių veiksmų buvo imtasi kibernetiniam incidentui suvaldyti ir užkirsti kelią panašioms įvykiams ateityje. ● Tolimesni žingsniai - informuoti apie būsimus veiksmus ir planus skirtus situacijai stabilizuoti ir atnaujinti organizacijos veiklą. 	List	
	<p>Kibernetinių incidentų analizė ir išmoktos pamokos</p> <p>Po kiekvieno kibernetinio incidento yra labai svarbu atlikti išsamią analizę ir nustatyti išmoktas pamokas. Šis procesas gali būti apibendrintas sekančiais žingsniais:</p> <ol style="list-style-type: none"> 1. Incidento analizė: <ul style="list-style-type: none"> ● Priežasčių nustatymas - nuodugnai ištirti, kas sukėlė kibernetinį incidentą, kokie pažeidžiamumai buvo išnaudoti ir kaip buvo vykdoma pati kibernetinė ataka. ● Incidento eiga - išsamiai dokumentuoti, kaip vystėsi kibernetinis incidentas nuo pradžios iki pabaigos, įskaitant visus veiksmus, kurių buvo imtasi jį suvaldyti. 2. Ataskaitos rengimas: <ul style="list-style-type: none"> ● Parengti išsamią ataskaitą, kurioje apibendrinami atlikto tyrimo rezultatai, kokios buvo nustatytos problemos ir pateikti rekomendacijos ateičiai. 3. Išmoktos pamokos: <ul style="list-style-type: none"> ● Procesų peržiūra - svarbu peržiūrėti ir atnaujinti esamus kibernetinio saugumo procesus ir procedūras remiantis incidento analizės rezultatais. ● Darbuotojų mokymas - suorganizuoti papildomus mokymus ir seminarus darbuotojams siekiant pagerinti jų žinias ir įgūdžius kibernetinio saugumo srityje. Labai pravartu yra naudoti konkrečius kibernetinių atakų pavyzdžius su kuriais organizacija buvo susidūrus ir kaip jie buvo suvaldyti. ● Periodiniai vertinimai - rekomenduojama reguliariai atlikti kibernetinio saugumo politikos ir procedūrų vertinimus atsižvelgiant į išmoktas pamokas ir nuolat besikeičiančias grėsmes. <p>Saugumo padėties gerinimas remiantis kibernetinio incidento išvadomis</p> <p>Remiantis kibernetinio incidento analizės išvadomis, organizacija turėtų imtis atitinkamų veiksmų saugumo padėčiai gerinti. Keletas iš potencialių veiksmų galėtų būti:</p>	Video	

	<ul style="list-style-type: none"> • Saugumo politikos atnaujinimas - reguliariai atnaujinti kibernetinio saugumo politiką įtraukiant naujas rekomendacijas ir gerąsias praktikas, kurios buvo nustatytos analizės metu. • Papildomų techninių priemonių diegimas ar jų atnaujinimas - patartina diegti pažangias įsibrovimų detektavimo ir prevencijos sistemas (IDS/IPS), SIEM (Security Information and Event Management) sistemas, ugniasienes ir kitas saugumo priemones. • Reguliari techninė priežiūra - svarbu užtikrinti, kad visos informacinės sistemos būtų nuolat prižiūrimos ir atnaujinamos siekiant apsaugoti nuo naujų grėsmių ar pažeidžiamumų. • Kibernetinio saugumo situacijos žinojimo gerinimas - diegti geopolitinės informacijos vertinimo mechanizmus ir sistemingą kibernetinių nusikaltėlių stebėseną. • Reakcijos laiko į kibernetines atakas gerinimas - atlikus kibernetinio incidento analizę ir aprašius išmoktas pamokas, reikėtų pasistengti įžvelgti kaip reakcijos laikas galėtų būti tobulintinas tam, kad kibernetiniai incidentai būtų greičiau ir efektyviau valdomi. • Rizikų valdymo gerinimas - sudaryti išsamų kibernetinio saugumo valdymo modelį, kuris integruotų svarbiausius atsparumo sisteminius ir valdymo faktorius. • Darbuotojų mokymai ir pratybos - skatinti darbuotojų mokymus, siekiant ugdyti kibernetinio saugumo kultūrą ir tinkamą kibernetinę higieną visais lygmenimis. 		
4.	Dirbtinis intelektas ir automatizavimas kibernetiniame saugume		
	<p>Šiuolaikinėje aplinkoje, kuri tampa vis labiau priklausoma nuo technologijų, kibernetinis saugumas yra esminis komponentas organizacijų veikloje. Kibernetinės grėsmės nuolat keičiasi ir tampa vis sudėtingesnės, todėl organizacijos turi būti pasirengusios reaguoti į naujus iššūkius. Kibernetinės atakos gali sukelti didelius finansinius nuostolius, sutrikdyti veiklą ir pakenkti reputacijai. Atsižvelgiant į šiuos iššūkius, dirbtinis intelektas (DI) ir automatizavimas tampa svarbiausiomis priemonėmis, galinčiomis padėti sustiprinti kibernetinį saugumą.</p> <p>Dirbtinis intelektas ir automatizavimas gali reikšmingai pagerinti kibernetinį saugumą, suteikdami galimybę greičiau ir tiksliau aptikti grėsmes, sumažinti žmogiškųjų klaidų tikimybę bei padidinti organizacijos atsparumą kibernetinėms grėsmėms. Vis dėlto, integruojant šias technologijas, būtina atsižvelgti į galimas rizikas ir iššūkius, tokius kaip technologijų spragos, privatumo klausimai ir etiniai svarstymai.</p> <p>Dirbtinio intelekto (DI) panaudojimo galimybės bei jo adaptacija įvairiose srityse vyksta labai sparčiai tiek pasauliniu, tiek Lietuvos mastu. Lietuvoje DI technologijos taip pat sparčiai tobulėja ir integruojamos į skirtingas sritis, atnešdamos reikšmingą naudą įvairiems sektoriams. 2024 m. gegužės 9 d. Lietuvos Respublikos Seimas priėmė Seimo</p>	V video	

	<p>rezoliuciją „Dėl dirbtinio intelekto technologijų naudojimo viešajame sektoriuje principų“ (Nr. XIVP-3717), kuri gali reikšmingai pakeisti valstybės požiūrį į dirbtinio intelekto (DI) politiką ir jo naudojimą viešajame sektoriuje.</p> <p>Citata - „Viešojo sektoriaus institucijos neapsieina be dirbtinio intelekto naudojimo. Jau dabar matome, kad dirbtinis intelektas įtraukia į įvairias veiklos sritis padėdamas optimizuoti procesus ir pagerinti rezultatus, suteikia naujų galimybių valstybės institucijoms ir viešojo administravimo subjektams veikti efektyviau, skaidriau ir atsakingiau. Tačiau tas dirbtinis intelektas yra naudojamas labai asmeniškai ir labai nereglamentuotai. Tai žmogus, naudojantis savo darbe dirbtinį intelektą, prisiima rizikas, visą atsakomybę. Taip galite ir duomenis nutekinti, taip galite ir netiksliai kažką tai padaryti. Jo tiesiog niekas neprižiūri. Norint užtikrinti, kad dirbtinio intelekto naudojimas atneštų visuomenei tik naudą, būtina numatyti vieningas teisinio reglamentavimo gaires“, – projekto pristatymo metu sakė jo iniciatorė Ateities komiteto Dirbtinio intelekto darbo grupės pirmininkė Rasa Petrauskienė.</p> <p>[Šaltinis - https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT(1).pdf]</p> <p>[Šaltinis - https://www.lrs.lt/sip/portal.show?p_r=35403&p_k=1&p_t=288543]</p> <p>[Šaltinis - https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/2ab5b621135e11ef8e4be9fad87afa59]</p> <p>Ši rezoliucija apibrėžia 11 principų, kurie turėtų būti taikomi dirbtinio intelekto integracijai į viešojo sektoriaus veiklą, siekiant užtikrinti skaidrumą, atsakomybę ir etikos standartus. Kiekvienam organizacijos vadovui svarbu būtų susipažinti su šiais principais, nesvarbu, ar dirbtinis intelektas būtų naudojamas kibernetinio saugumo lygio gerinimui, ar kitais aspektais.</p>		
4.1.	Dirbtinio intelekto ir automatizavimo vaidmuo		
	<p>Dirbtinis intelektas ir automatizavimas gali žymiai pagerinti kibernetinį saugumą keliais būdais. Visų pirma, DI technologijos gali aptikti grėsmes realiuoju laiku, naudodamos pažangias mašininio mokymosi (MM) technologijas. MM modeliai yra treniruojami su dideliais duomenų rinkiniais, kad galėtų atpažinti anomalijas ir neįprastą veiklą, kuri gali rodyti kibernetinį išpuolį. Šios technologijos gali aptikti ne tik žinomus grėsmių modelius, bet ir naujas, dar neaptiktas grėsmes, kurios gali būti praleistos tradiciniais metodais.</p>	Video	

	<p>Pavyzdys: Naudojant atviro kodo įrankį „Elastic Stack“ su mašininio mokymosi papildiniu „X-Pack“, galima realiuoju laiku analizuoti žurnalų įrašus ir aptikti anomalijas, kurios gali rodyti kibernetinę grėsmę.</p> <p>SOC (Saugumo operacijų centras) veiklos efektyvumas taip pat gali būti žymiai pagerintas naudojant automatizuotas užduočių vykdymo sistemas. Šios sistemos gali automatiškai analizuoti įspėjimus, nustatyti jų prioritetus ir vykdyti automatizuotas reagavimo procedūras. Tai leidžia analitikams susitelkti į sudėtingesnes ir strategines užduotis, o ne į pasikartojančius, laiko reikalaujančius darbus. Automatizavimas taip pat padeda sumažinti žmogiškųjų klaidų riziką, nes standartizuoti atsakymo scenarijai užtikrina, kad visos procedūros bus vykdomos nuosekliai ir tiksliai.</p> <p>Pavyzdys: Naudojant atviro kodo SOAR platformą „TheHive“, organizacijos gali automatizuoti incidentų valdymo procesus nuo aptikimo iki reagavimo, integruojant įvairius saugumo įrankius ir duomenų šaltinius.</p> <p>Be to, DI technologijos gali padėti geriau suprasti kibernetinių grėsmių kraštovaizdį, analizuodamos didelius duomenų kiekius ir identifikuojamos tendencijas bei grėsmių modelius. Tai leidžia organizacijoms būti proaktyviomis ir imtis prevencinių priemonių, o ne reaguoti tik po to, kai grėsmė jau pasireiškė. DI taip pat gali padėti optimizuoti išteklių naudojimą, nustatant sritis, kuriose reikia daugiau dėmesio ir investicijų.</p> <p>Mašininis mokymasis (angl. „Machine Learning“) yra technologija, kuri yra sudedamoji Dirbtinio intelekto (angl. „Artificial Intelligence“ arba santrumpa „AI“) dalis. Mašininio mokymosi (MM) modeliai yra kita svarbi technologija, naudojama kibernetiniame saugume. Šie modeliai gali būti pritaikyti įvairioms saugumo užduotims, tokioms kaip klasifikacija (pvz., kenkėjiškos programos atpažinimas), regresija (pvz., grėsmių prognozavimas) ir klasterizacija (pvz., panašių incidentų grupavimas). MM modeliai yra treniruojami naudojant didelius duomenų rinkinius, kad galėtų atpažinti sudėtingus grėsmių modelius ir tendencijas. Šios technologijos gali būti ypač naudingos aptinkant nežinomas ar naujas grėsmes, kurios gali būti praleistos tradiciniais metodais.</p> <p>Kiti dirbtinio intelekto įrankiai, tokie kaip natūralios kalbos apdorojimo (NLP) ar vaizdų atpažinimo technologijos, taip pat yra naudojami kibernetiniame saugume. NLP technologijos gali būti naudojamos grėsmių aptikimui iš tekstinių duomenų, tokių kaip žurnalų įrašai, socialinių tinklų žinutės ar elektroniniai laiškai. NLP gali padėti analizuoti didelius tekstinių duomenų kiekius ir identifiкуoti potencialias grėsmes ar anomalijas. Vaizdų atpažinimo technologijos gali būti naudojamos aptinkant ir analizuojant vaizdinę informaciją, pavyzdžiui, stebėjimo kamerų įrašus, siekiant aptikti neįprastą veiklą ar potencialias grėsmes.</p>		
4.2.	Dirbtinio intelekto sprendimų įgyvendinimas		

<p>Integruojant dirbtinį intelektą į esamą saugumo infrastruktūrą, svarbu pradėti nuo strateginio plano kūrimo. Tai apima tikslų nustatymą, esamos infrastruktūros analizę ir pasiruošimą pokyčiams. Svarbu įvertinti, kaip DI ir automatizavimas gali papildyti esamas saugumo priemones ir kokie resursai reikalingi jų sėkmingam įgyvendinimui.</p> <p>Pirmasis žingsnis yra atlikti esamos saugumo infrastruktūros analizę, kad būtų galima nustatyti silpnąsias vietas ir sritis, kuriose DI ir procesų automatizavimas gali suteikti didžiausią vertę. Tai apima esamų saugumo priemonių ir procesų vertinimą, siekiant nustatyti, kur galima pagerinti efektyvumą ir sumažinti riziką. Taip pat svarbu nustatyti tikslus ir lūkesčius, susijusius su DI ir automatizavimo integravimu, siekiant užtikrinti, kad visi suinteresuotieji asmenys yra susipažinę su projekto tikslais ir yra pasirengę pokyčiams.</p> <p>Palaipsninis įdiegimas ir testavimas yra esminis etapas, siekiant užtikrinti, kad naujos technologijos bus veiksmingos ir patikimos. Pilotiniai projektai leidžia išbandyti DI sprendimus mažesniu mastu ir įvertinti jų efektyvumą prieš plačiau juos diegiant. Tai taip pat suteikia galimybę identifikuoti ir spręsti problemas bei iššūkius, kurie gali kilti diegiant naujas technologijas. Svarbu išlaikyti lankstumą ir gebėti prisitaikyti prie naujų iššūkių bei poreikių.</p> <p>Pavyzdys: Organizacija gali pradėti pilotinį projektą, naudodama „TheHive“ platformą, siekdama automatizuoti incidentų valdymo procesus. Projektas gali būti vykdomas ribotoje aplinkoje, siekiant įvertinti efektyvumą ir nustatyti galimus patobulinius prieš platesnį sprendimo diegimą.</p> <p>Komandos mokymas ir kompetencijų ugdymas yra kitas svarbus aspektas. Specialistų rengimas ir jų žinių tobulinimas padeda užtikrinti, kad organizacijos darbuotojai sugebės efektyviai naudotis DI ir automatizavimo priemonėmis. Tai apima mokymus apie naujas technologijas, jų naudojimą ir geriausias praktikas. Taip pat svarbu skatinti tarpdisciplininį bendradarbiavimą, siekiant integruoti įvairių sričių žinias ir patirtį. Tai padeda užtikrinti, kad visi suinteresuotieji asmenys yra pasirengę dirbti su naujosiomis technologijomis ir efektyviai jas taikyti.</p> <p>Įgyvendinant dirbtinio intelekto sprendimus, susiduriama su įvairiais technologiniais ir organizaciniais iššūkiais. Technologiniai iššūkiai apima duomenų kokybės ir prieinamumo problemas, modelių interpretaciją ir aiškinimą. Organizaciniai iššūkiai gali būti susiję su pasipriešinimu pokyčiams, kultūrinėmis kliūtimis ir biudžeto paskirstymo problemomis.</p> <p>Etiniai ir teisiniai svarstymai taip pat yra svarbūs. Dirbtinio intelekto sprendimų skaidrumas ir atsakomybė, duomenų privatumo apsauga ir atitikties reikalavimai yra pagrindiniai aspektai, kuriuos būtina apsvarstyti diegiant naujas technologijas.</p>	<p>Video</p>	
--	--------------	--

	<p>Įmonės vadovai turi užtikrinti, kad DI sprendimai būtų skaidrūs ir atskaitingi. Tai reiškia, kad modeliai turi būti interpretuojami ir paaiškinami, siekiant užtikrinti, kad sprendimai būtų priimami remiantis patikimais duomenimis ir pagrįstais modeliais. Tai taip pat apima etinių principų laikymąsi ir atitikimą teisės aktų reikalavimams.</p> <p>Ateities tendencijos ir galimybės kibernetiniame saugume rodo, kad DI ir automatizavimas toliau vystysis ir taps vis svarbesniais įrankiais kovojant su kibernetinėmis grėsmėmis. Inovacijų kryptys ir nauji technologiniai sprendimai padės organizacijoms efektyviau apsaugoti savo duomenis ir sistemas.</p> <p>Sėkmės istorijos ir pavyzdžiai iš rinkos lyderių gali būti naudingos siekiant įkvėpti ir parodyti praktinius žingsnius sėkmingam DI ir automatizavimo diegimui. Nuolatinis mokymasis ir prisitaikymas prie besikeičiančių grėsmių ir technologijų yra esminis aspektas kibernetinio saugumo srityje.</p>		
5.	Modulio (kurso) žinių patikrinimo testas		
	<p>Sujungti poras Klausimas - sujungite atitinkamas grėsmių modeliavimo ir vertinimo sistemų poras</p> <ul style="list-style-type: none"> ● STRIDE -> Skirtas nustatyti galimas saugumo grėsmes programinės įrangos kūrimo projektavimo etape. ● DREAD -> Skirtas kiekybiškai įvertinti ir nustatyti prioritetinėms kibernetinio saugumo rizikoms ● PASTA -> Skirtas kibernetinių grėsmių nustatymui, analizavimui ir jų suskirstymui pagal svarbą ● LINDDUN -> Skirtas duomenų privatumo pažeidžiamumams nustatyti ● OCTAVE -> Skirtas prioritetizuoti ir valdyti informacinio saugumo rizikas <p>Keli teisingi atsakymai Klausimas - kokie trys pagrindiniai aspektai padeda užtikrinti kibernetinį saugumą?</p> <ul style="list-style-type: none"> ● Konfidencialumas (Teisingas) ● Vientisumas (Teisingas) ● Prieinamumas (Teisingas) ● Privatumas (Neteisingas) ● Slaptažodžiai (Neteisingas) <p>Vienas teisingas atsakymas Klausimas - Kibernetinio Saugumo būklė vs kibernetinio saugumo atitiktis</p>		

	<ul style="list-style-type: none"> • Saugumo atitiktis išreiškia priemones, kurias organizacija įgyvendina, kad atitiktų sutartinius arba reguliacinius reikalavimus. Kibernetinio saugumo būklė apima kibernetinės apsaugos priemones ar sprendimus, kurias organizacija taiko, siekdama apsaugoti savo IT turtą, duomenis ir klientus. (Teisingas) • Saugumo atitiktis apima tik technines apsaugos priemones, tokias kaip ugniasienės ir antivirusinės programos. Kibernetinio saugumo būklė yra susijusi su organizacijos finansiniais ištekliais, skirtais IT sistemų atnaujinimui. (Neteisingas) • Saugumo atitiktis reiškia organizacijos gebėjimą apsaugoti savo klientų asmeninius duomenis nuo viešinimo. Kibernetinio saugumo būklė apima tik organizacijos gebėjimą aptikti kibernetines grėsmes realiuoju laiku. (Neteisingas) <p>Vienas teisingas atsakymas</p> <p>Klausimas - Kuris variantas NĖRA vienas iš rizikos mažinimo strategijų</p> <ul style="list-style-type: none"> • Rizikos vengimas • Rizikos ignoravimas (Teisingas) • Rizikos perkėlimas • Rizikos priėmimas <p>Vienas teisingas atsakymas</p> <p>Koks yra pagrindinis privalumas naudojant mašininio mokymosi technologijas kibernetinio saugumo srityje?</p> <p>A) Galimybė automatiškai generuoti vartotojų slaptažodžius.</p> <p>B) Galimybė realiuoju laiku aptikti grėsmes ir anomalijas. (Teisingas)</p> <p>C) Galimybė pakeisti organizacijos IT infrastruktūrą.</p> <p>D) Galimybė sumažinti duomenų atsargų kiekį.</p> <p>Vienas teisingas atsakymas</p> <p>Kodėl svarbu atlikti pilotinį projektą prieš diegiant dirbtinio intelekto sprendimus plačiu mastu?</p> <p>A) Siekiant sumažinti IT technologijų diegimo kainą.</p> <p>B) Siekiant išbandyti sprendimus mažesniu mastu ir įvertinti jų efektyvumą. (Teisingas)</p> <p>C) Siekiant padidinti darbuotojų darbo našumą.</p> <p>D) Siekiant sumažinti duomenų saugumo reikalavimus.</p>		
6.	Kurso santrauka, rekomendacijos (PDF), max 1 l.		

<p>Kibernetinis saugumas – tai veiksmai, kurių imamasi norint apsaugoti kibernetinę aplinką ir užtikrinti informacinėmis sistemomis perduodamus ar jose tvarkomos elektroninės informacijos prieinamumą, vientisumą bei konfidencialumą.</p> <p>Pasiekti 100% kibernetinį saugumą yra neįmanoma dėl nuolat besikeičiančių grėsmių, žmogaus klaidų ir sudėtingų IT sistemų. Nors visiškas saugumas nepasiekiamas, organizacijos gali sumažinti riziką taikydamos prevencines, detektavimo ir atsakomąsias priemones bei nuolatinę stebėseną ir atnaujinimus.</p> <p>Pagrindiniai kibernetinio saugumo principai</p> <ul style="list-style-type: none"> • Konfidencialumas - informacija prieinama tik tiems asmenims, kurie turi teisę ją matyti. Konfidencialumo užtikrinimas apima prieigos kontrolės mechanizmus, šifravimą ir kitus metodus, apsaugančius informaciją nuo neteisėtos prieigos. • Vientisumas - informacija tiksli ir nepakeista, išskyrus įgaliotus pakeitimus. Vientisumo užtikrinimas apima apsaugą nuo neteisėto duomenų keitimo - tiek tyčinio, tiek atsitiktinio. • Prieinamumas - informacija ir informacinės sistemos yra pasiekiamos tada, kai jų reikia. Užtikrinant prieinamumą, svarbu apsaugoti sistemas nuo gedimų, paskirstytų paslaugos trikdymo atakų (DDoS) ir kitų trikdžių, kurie gali sutrikdyti paslaugų teikimą. <p>Kibernetinio saugumo reikalavimai organizacijai</p> <ul style="list-style-type: none"> • Politikos ir procedūros - formaliai apibrėžtos saugumo politikos ir procedūros, įskaitant incidentų reagavimo planus ir duomenų apsaugos planus. • Techninės kontrolės priemonės - ugniasienės, įsilaužimų aptikimo sistemos (IDS), šifravimo metodai, prieigos kontrolės mechanizmai. • Fizinis saugumas - prieigos kontrolės sistemos ir stebėjimas, siekiant išvengti neteisėtos fizinės prieigos prie kritinės infrastruktūros. • Žmogiškieji veiksniai - nuolatinis darbuotojų mokymas ir kibernetinio saugumo sąmoningumo didinimas visais organizacijos lygmenimis. • Stebėjimas ir aptikimas - nuolatinis IT sistemų stebėjimas naudojant SIEM įrankius. • Incidentų reagavimas ir atkūrimas - išsamūs incidentų reagavimo ir veiklos tęstinumo planai. <p>Kibernetinio saugumo teisinė atsakomybė</p>		
--	--	--

<p>Lietuvos Respublikos kibernetinis saugumas apima bendriausias sritis, tokias kaip kibernetinio saugumo politikų nustatymas, kibernetinė higiena, bet taip pat ir siauresnius ir konkretesnius reikalavimus, pvz., kriptografijos ar prieigų valdymo sritis. Šie reikalavimai laikomi minimaliais. Organizacijos gali nustatyti papildomus reikalavimus, atsižvelgdamos į jų veiklai kylančias grėsmes. Kitas labai svarbus aspektas yra tas, kad įstatymas <u>nustato pareigą paskirti už kibernetinį saugumą atsakingus asmenis(-i) organizacijoje, taip pat numato tiesioginę organizacijos vadovo atsakomybę už kibernetinį saugumą, nustatant tiesiogines, tik vadovui skirtas pareigas.</u></p> <p>Dėmesio reikėtų skirti ir esamiems, ir būsimiems reglamentams bei teisės aktams:</p> <ul style="list-style-type: none"> ● BDAR (Bendrasis duomenų apsaugos reglamentas) - nustato asmens duomenų tvarkymo ir saugumo reikalavimus. ● TIS 2 (Tinklų ir informacinių sistemų direktyva) - siekiama užtikrinti aukštą tinklų ir informacinių sistemų saugumo lygį ES valstybėse narėse, ypačingai tų subjektų, kurie teikia esmines paslaugas visuomenei ir ekonomikai. <ul style="list-style-type: none"> ○ Organizacijų kibernetinis saugumas - TIS2 orientuojasi į organizacijų ir paslaugų teikėjų kibernetinio saugumo priemonių įgyvendinimą. ○ Kritinės infrastruktūros apsauga: Daugiausia dėmesio skiriama kritinės infrastruktūros, kurios veiklos sutrikimai gali turėti didelį poveikį visuomenei ir ekonomikai, apsaugai. ● CRA (Cyber Resilience Act) - siekiama padidinti kibernetinio saugumo lygį, užtikrinant, kad visos skaitmeninės prekės ir paslaugos, teikiamos Europos Sąjungoje, atitiktų kibernetinio saugumo reikalavimus. <ul style="list-style-type: none"> ○ Produkto kibernetinis saugumas: CRA daugiausia dėmesio skiria tam, kad visos skaitmeninės prekės ir paslaugos būtų saugios nuo kibernetinių grėsmių nuo pat jų kūrimo momento. ○ Gamintojų ir tiekėjų atsakomybė: reguliuoja gamintojų ir tiekėjų atsakomybę už skaitmeninių prekių ir paslaugų saugumą. <p>Rizikos valdymas</p> <ul style="list-style-type: none"> ● Rizikos identifikavimas - potencialių rizikų nustatymas. ● Rizikos vertinimas - rizikų poveikio ir tikimybės analizė. ● Rizikos mažinimas - veiksmų plano kūrimas ir įgyvendinimas. ● Rizikos stebėseną ir kontrolę - nuolatinis rizikos valdymo proceso peržiūrėjimas ir koregavimas. <p>Kibernetinio saugumo metrikos</p>		
---	--	--

	<ul style="list-style-type: none"> • Metrikų nustatymas - bandymų įsilaužti į sistemas kiekis, nustatytų pažeidžiamumų skaičius, darbuotojų mokymų rodikliai. • Metrikų stebėjimas ir vertinimas - nuolatinė stebėsena ir vertinimas siekiant gerinti kibernetinio saugumo būklę. <p>Dirbtinis intelektas ir automatizavimas kibernetiniame saugume</p> <p>Dirbtinis intelektas ir automatizavimas kibernetiniame saugume padeda greitai aptikti ir analizuoti grėsmes, sumažinti žmogiškųjų klaidų tikimybę, optimizuoti saugumo priemones ir automatizuoti pasikartojančius procesus, tokius kaip pažeidžiamumų skenavimas ir taisymas, taip didinant saugumo valdymo efektyvumą ir atsparumą kibernetinėms atakoms.</p> <p>Tačiau svarbiausia paminėti, kad Lietuvos Respublikos Seimas yra priėmęs Seimo rezoliuciją „Dėl dirbtinio intelekto technologijų naudojimo viešajame sektoriuje principų“, kuri apibrėžia 11 principų, kurie turėtų būti taikomi dirbtinio intelekto integracijai į viešojo sektoriaus veiklą.</p>		
7.	Šaltiniai		
	https://www.nksc.lt/doc/akreditacija/duk_informacines_sistemas.pdf https://www.nksc.lt/doc/Kibernetinio_saugumo_vadovas_verslui_2020.pdf https://www.nksc.lt/doc/NKSC%20plakatas%20(20cc)_1.pdf https://www.nksc.lt/rekomendacijos/interneto_svetainiu_apsauga.html https://data.kurkl.lt/wp-content/uploads/2023/04/SVV-kibernetinio-saugumo-apklauso-apzvalga-Kurk-Lietuvai.pdf https://luminor.lt/lt/naujienos/tyrimas-lietuvas-verslas-savo-kibernetiniu-saugumu-rupinasi-maziausiai-is-baltijos-saliu https://nordpass.com/most-common-passwords-list/ https://www.nksc.lt/aktualu.html https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/ITpnlvtcfz https://vdai.lrv.lt/lt/naujienos/pokyciai-lietuvas-respublikos-asmens-duomenu-teisines-apsaugos-istatyme/ https://vdai.lrv.lt/uploads/vdai/documents/files/el_ASMENS%20DUOMEN%C5%B2%20APSAUGA%20DARBO%20SANTYKI%C5%B2%20KONTEKSTE%20Gair%C4%97s%20smulkiajam%20ir%20vidutiniam%20verslui.pdf		

https://vdai.lrv.lt/uploads/vdai/documents/files/01_%20SolPriPa%20Asmens%20duomenu%20apsaugos%20gaires%20SMULKIAJAM%20IR%20VIDUTINIAM%20VERSLUI%202019-11-08.pdf https://kam.lt/tinklu-ir-informaciniu-sistemu-direktyva/ https://www.nksc.lt/doc/rizikos_analize.pdf https://cris.mruni.eu/cris/entities/etd/a611e234-8754-4256-926c-fa5d7b551dc3 https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/cbddab726c5b11eea182def3ac5c11d6?positionInSearchResults=0&searchModelUUID=b95cc445-ea54-4923-b05e-1c257bbbccbb https://www.cisecurity.org/controls/cis-controls-self-assessment-tool-cis-csat https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html https://threat-modeling.com/linddun-threat-modeling/ https://threat-modeling.com/dread-threat-modeling/ https://owasp.org/www-community/Threat_Modeling_Process https://www.iriusrisk.com/resources-blog/threat-modeling-methodology-stride https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT(1).pdf https://www.lrs.lt/sip/portal.show?p_r=35403&p_k=1&p_t=288543 https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/2ab5b621135e11ef8e4be9fad87afa59		
---	--	--