Kibernetinio saugumo reikalavimai ir jų įgyvendinimas praktikoje (LŠTA)

prof. dr. Darius Štitilis

2022-03-28

Įvadiniai aspektai

• Kibernetinio saugumo reikalavimai įmonėms/organizacijoms **griežtėja**, jų daugėja. Reguliavimo našta didėja.

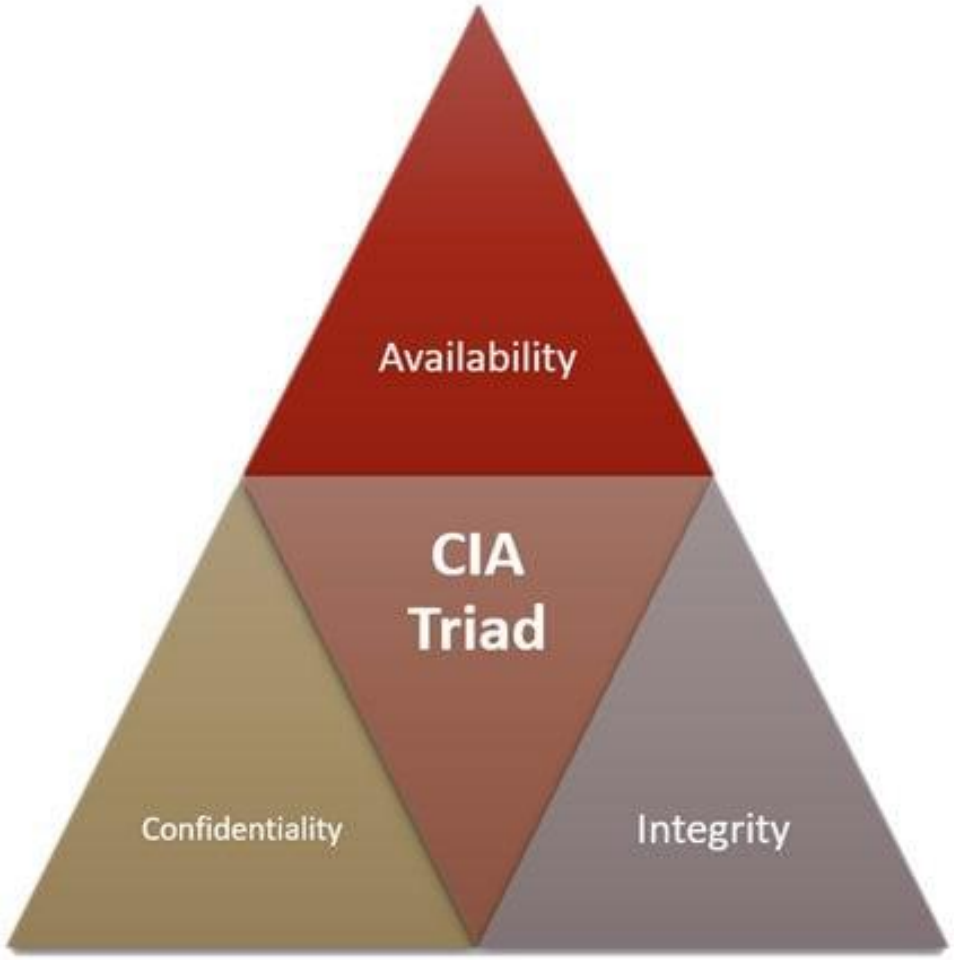
• Daugėja reguliuojamų subjektų. Dalis subjektų nežino, kad yra/kaip yra reguliuojami. **Subjektui yra vis dar sunku įvertinti ar yra reguliuojamas**.

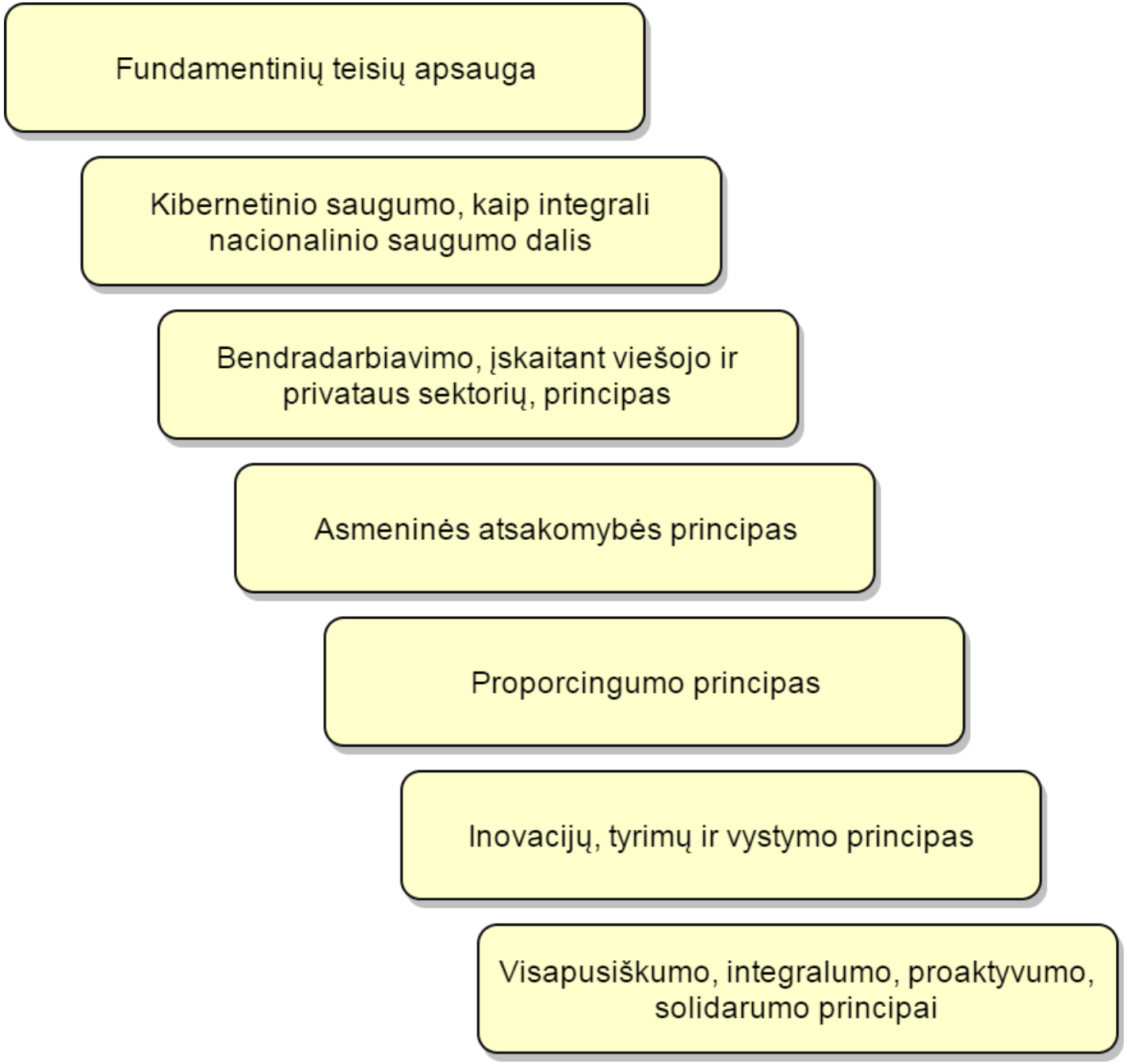
• Reguliavimas ir kontrolė sutelkti į „vienas rankas“ (**vienoje sistemoje**). Situacija NKSC.

• Į neatitikimą reikalavimams reaguojama vis griežčiau, tolerancijos kartelė žemėja.

• Vis dar yra taikomi net keli institutai, susiję su sauga:

- **El. informacijos sauga** - elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas.
- **Kibernetinis saugumas** - visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą.


Availability
CIA
Triad
Confidentiality
Integrity


Fundamentinių teisių apsauga
Kibernetinio saugumo, kaip integrali nacionalinio saugumo dalis
Bendradarbiavimo, įskaitant viešojo ir privataus sektorių, principas
Asmeninės atsakomybės principas
Proporcingumo principas
Inovacijų, tyrimų ir vystymo principas
Visapusiškumo, integralumo, proaktyvumo, solidarumo principai

KIBERNETINIO SAUGUMO GRĖSMĖS, TENDENCIJOS

- Statistiškai incidentų mažėja, tačiau atakos – labiau rafinuotos.
- Grėsmės – dėl didelio skaičiaus prie interneto prijungtų neapsaugotų įrenginių, pažeidžiamų interneto svetainių ir piktavališkų socialinės inžinerijos metodų naudojimo (pastarųjų – 25% daugiau nei 2017 m.).
- YSII – aktvios kibernetinės veiklos objektas (kenkimo PĮ, išaugusi žvalgybos veikla).
- Neigiama informacinė veikla nutaikyta į svarbiausias nacionalinio saugumo sritis. Trečdalis informacinių atakų – gynybos srityje.
- Rezonansiniai hibridiniai incidentai (*hibridinis karas?*).
- Rangovų patikimumo klausimas.
- Įrenginių saugumas.
- (*sertifikavimas?*).

- Lietuvoje **nepakankamai vertinamas kibernetinių incidentų poveikis**. https://kaunas.kasvyksta.lt/, „Kauno vandenų pavyzdžiai.
- Viešajame sektoriuje **interneto svetainių** kibernetinio saugumo būklė gerėja, bet reikšmingos rizikos išlieka.
- **Formalios atitikties problema**: Formalus kibernetinio saugumo reikalavimų įgyvendinamas didėja, tačiau kyla keblumų diegiant praktines kibernetinių incidentų rizikų kontrolės priemones.
- **Hibridiniai incidentai**, susidedantys iš informacinės ir kibernetnės dalies: *kibernetinio saugumo požiūriu incidentai nebuvo rafinuoti, tačiau iš informacinės pusės buvo siekiama rezonanso eskaluojant ir didinant melagingos informacijos sklaidą*.

- **Kibernetinio saugumo rizikos didėjo** (daugiausia dėl Covid išaugo online paslaugų poreikis).
- **NKSC patikrinimai**: tikrinti 6 kibernetinio saugumo subjektai, valdantys VII ir YSII:
  - Reikalavimų įgyvendinimo procesas vis dar lėtas;
  - Aplaidus VII valdytojų požiūris.
- **Nesaugios interneto svetainės** (*prasta priežiūra, neatnaujinamos turinio valdymo sistemos (TVS), vieša prieiga prie svetainių TVS ir nesaugūs slaptažodžiai*).
- **Nesaugios įrangos ir technologijų naudojimas didina kibernetinio saugumo rizikas**.
- **RIS spragų atskleidimo praktika** – vienas iš efektyvių būdų stiprinti kibernetinį saugumą.

- Didžioji dalis kibernetinėje erdvėje priešiškos veiklos susijusi su Rusija.
- Bandyta veikti rinkimus ir per kibernetines atakas;
- KIBERNETINIS ŠNIPINĖJIMAS.
- Aktyvi su Rusija siejamų grupuočių veikla: orientuojamasi į karinio, ekonominio ir politinio pobūdžio informacijos rinkimą Lietuvos ir NATO IT infrastruktūroje.
- Kenkėjiškam kodui platinti naudojama socialinė inžinerija.
- Duomenų nutekinimo grėsmė naudojantis rusiškais tinklais ir el. pašto paslaugomis.

ANTRASIS
OPERATYVINIŲ
TARNYBŲ
DdepartamentAS
PRIE KRAŠTO
APSAUGOS
MINISTERIJOS

LIETUVOS
RESPUBLIKOS
VALSTYBĖS
SAUGUMO
DEPARTAMENTAS

GRĖSMIŲ NACIONALINIAM SAUGUMUI VERTINIMAS 2020

- Lietuvos kibernetinėje erdvėje pastebima **tęstinė kenkėjiška Rusijos ir Kinijos kibernetinių pajėgumų veikla**.
- Iš Rusijos, Kinijos ir kitų valstybių **vykdoma techninė informacinių sistemų žvalgyba**.
- Fiksuojami **bandymai gauti prieigas** prie valstybinės ypatingos svarbos infrastruktūros bei prie privataus sektoriaus informacinių sistemų ir panaudoti jas šnipinėjimui.
- **Didžiausią grėsmę** Lietuvos informacinių sistemų ir jose laikomos informacijos saugumui kelia **Rusijos žvalgybos tarnybų kibernetinis šnipinėjimas**.
- **Informacinės-kibernetinės operacijos** prieš Lietuvą.

- **Rusijos žvalgybinė veikla** prieš Lietuvą **išlieka intensyvi**. Per COVID-19 pandemiją išaugo kibernetinio šnipinėjimo grėsmė. Grėsmės padidėjimas siejamas su **padidėjusiais nuotolinio darbo ir elektroninių paslaugų mastais**.
- **Didžiausią grėsmę** Lietuvos institucijoms kelia **Rusijos žvalgybos tarnybų koordinuojamos kibernetinio šnipinėjimo grupuotės.**
- **Daugėja prieš Lietuvą nukreiptų informacinių-kibernetinių atakų**. Dezinformacijos sklaida ir kibernetinės manipuliacijos vienu metu įgyvendinamos Lietuvoje ir kaimyninėse šalyse. Atakomis siekiama silpninti transatlantinius ryšius, skaldyti visuomenę ir skatinti jos nepasitikėjimą institucijomis.
- 2020 m. fiksuotas **didesnis informacinių-kibernetinių operacijų** prieš Lietuvą **skaičius**.

Saugos konsolidacija

- Valstybės kibernetinio saugumo išteklių konsolidacija:
  - KAM (kibernetinės ir elektroninės informacijos saugos funkcijų ir tarnybų konsolidavimas).
  - NKSC („Vieno langelio principas“).
  - RRT CERT prijungimas.
- Kibernetinio saugumo pajėgumų konsolidacija – VĮ „Infostruktūra“ (SVDPT) „perdavimas“ KAM. Nuo 2019-07-01 – **Kertinis valstybės telekomunikacijų centras (KVTC)** (*2019 m. kovo 6 d. LRV nutarimas Nr. 12-01-383*)
- „**Saugiojo tinklo naudotojų sąrašas**“, LRV nutarimas 2019-05-22 Nr. 504 (*valst. institucijos, savivaldybės, ligoninės, priešgaisrinės apsaugos tarnybos ir kt.* (iš viso apie 463, atitikti org.-tech. reikalavimus „privalo“ tik apie 320)). 2020-10-21 paskutinė redakcija.

Dėl Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo įgyvendinimo saugiojo valstybinio duomenų perdavimo tinkl srityje

Rūšis:	Nutarimas
Identifikacinis kodas:	2018-00362
Užregistravimo TAR data:	2018-01-09
Galioja	Įsigalioja 2018-01-10

Priėmimo data:	2018-01-03
Įstaigos suteiktas nr.:	27
Priėmė:	Lietuvos Respublikos Vyriausybė
Paskelbta:	TAR, 2018-01-09, Nr. 362

Galiojanti suvestinė redakcija:	2020-10-21 -
Suvestinių redakcijų sąrašas pagal datą:	
Pakeitimų projektai:	Nėra
Eurovoc terminai:	
Ryšys su ES teisės aktais:	Nėra

Galiojanti suvestinė redakcija (nuo 2020-10-21)

DOCX ODT PDF

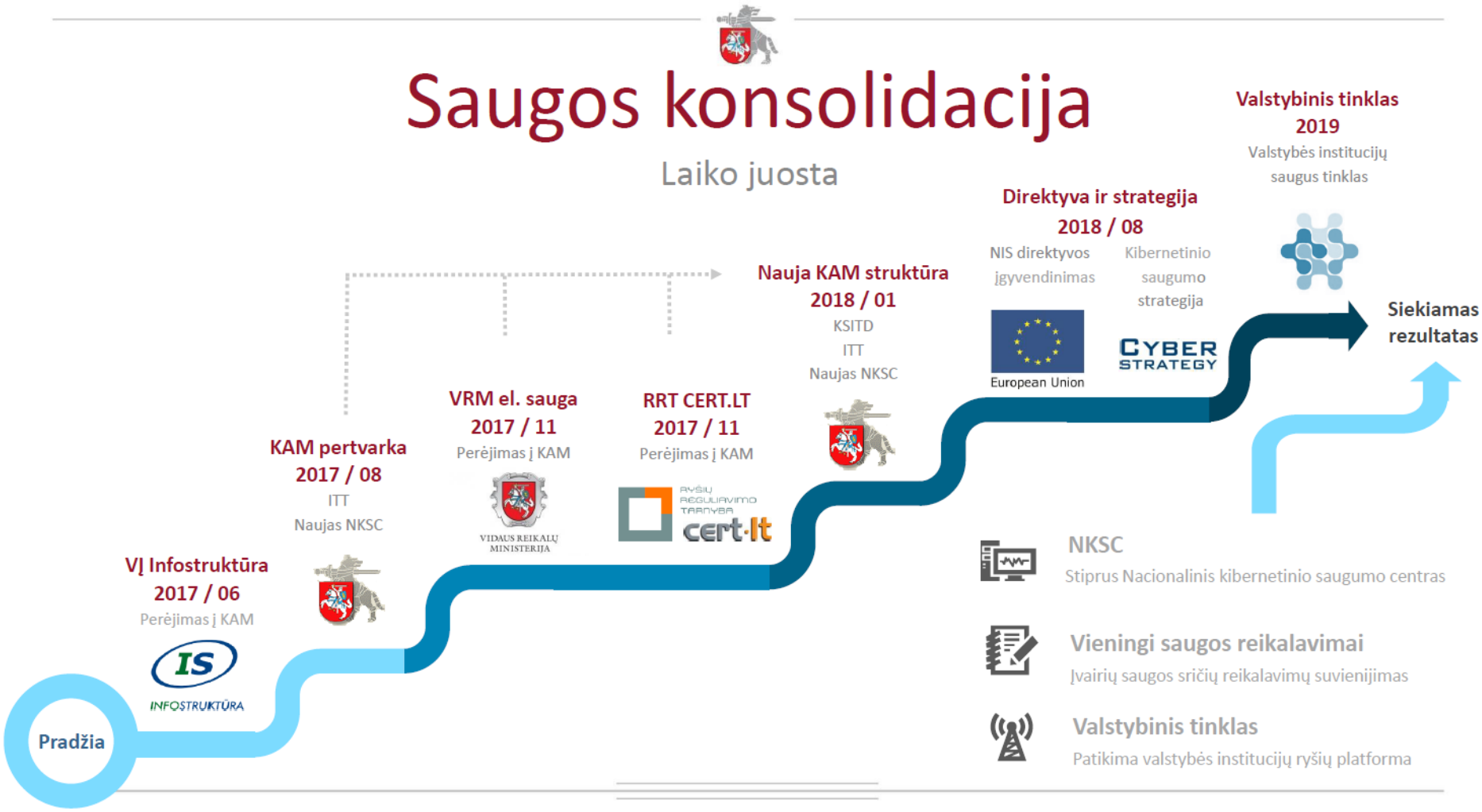
257.	Ignalinos rajono priešgaisrinė tarnyba
258.	Ignalinos rajono savivaldybės administracija
259.	Viešoji įstaiga „Ignalinos rajono ligoninė“
Jonavos rajono savivaldybė	
260.	Jonavos rajono priešgaisrinė tarnyba
261.	Jonavos rajono savivaldybės administracija
262.	Viešoji įstaiga Jonavos greitosios medicinos pagalbos stotis
263.	Viešoji įstaiga Jonavos ligoninė
264.	Viešoji įstaiga Jonavos pirminės sveikatos priežiūros centras
Joniškio rajono savivaldybė	
265.	Joniškio rajono savivaldybės administracija
266.	Joniškio rajono savivaldybės priešgaisrinė tarnyba
267.	Viešoji įstaiga Joniškio ligoninė
268.	Viešoji įstaiga Joniškio rajono savivaldybės greitosios medicinos pagalbos stotis
Jurbarko rajono savivaldybė	
269.	Jurbarko rajono priešgaisrinė tarnyba
270.	Jurbarko rajono savivaldybės administracija

Susijusi informacij

- Teisės akto pakeitimai (9)
- Susiję dokumentai (3)

Saugos konsolidacija

Laiko juosta



https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f?jfwid=dg8d31595

Pradžia | Paieška | Vertinimų vidurkis: 5 | LT

Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo

Rūšis:	Nutarimas	Priėmimo data:	2018-08-13	**Galiojanti suvestinė redakcija:**	2019-01-01 -
Identifikacinis kodas:	2018-13252	Dokumento nr.:	818	Suvestinių redakcijų sąrašas pagal datą:	
Užregistravimo TAR data:	2018-08-21	Priėmė:	Lietuvos Respublikos Vyriausybė	Pakeitimų projektai:	Nėra
Galioja	Įsigalioja 2018-08-22	Paskelbta:	TAR, 2018-08-21, Nr. 13252	Eurovoc terminai:	
Kalba:	Lietuvių			Ryšys su ES teisės aktais:	Nėra

Dokumento struktūra

Teisės akto tekstas (Nuorašas:)

LIETUVOS RESPUBLIKOS VYRIAUSYBĖ

NUTARIMAS
DĖL NACIONALINĖS KIBERNETINIO SAUGUMO STRATEGIJOS PATVIRTINIMO

2018 m. rugpjūčio 13 d. Nr. 818
Vilnius

Vadovaudamasi Lietuvos Respublikos kibernetinio saugumo įstatymo 5 straipsnio 1 punktu ir įgyvendindama Europos Parlamento ir Tarybos direktyvos 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (OL 2016 L 194, p. 1) 7 straipsnio 1 dalį, Lietuvos Respublikos Vyriausybė n u t a r i a:

1. Patvirtinti Nacionalinę kibernetinio saugumo strategiją (pridedama).
2. Pavesti Lietuvos Respublikos krašto apsaugos ministerijai iki 2018 m. lapkričio 2 d. pateikti Lietuvos Respublikos Vyriausybei tvirtinti Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinį veiklos plano projektą.
3. Pasiūlyti nevyriausybinėms organizacijoms, suinteresuotiems viešojo ir privataus sektorių atstovams, Lietuvos mokslo ir studijų institucijoms dalyvauti įgyvendinant Nacionalinę kibernetinio saugumo strategiją.

Susijusi informacija

- Teisės akto pakeitimai (1)
- Susiję dokumentai (3)

Lietuvos Respublikos nacionalinės kibernetinio saugumo strategijos tikslai ir uždaviniai

Stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą	Užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją, užkardymą ir tyrimą	Skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą	Stiprinti glaudų viešojo ir privataus sektoriaus bendradarbiavimą	Stiprinti tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų KS srityje vykdymą
Kurti sisteminį požiūrį į KS ir prevencinę veiklą	Plėtoti valstybės pajėgymus ir gebėjimus kovoti su EN	Plėtoti mokslinius tyrimus ir pridėtinės vertės veiklas KS	Gerinti bendradarbiavimo koordinavimą	Plėtoti įvairių lygių bendradarbiavimą
Didinti KS politikos formav. ir įgyvendinimo efektyvumą	Stiprinti EN prevenciją ir kontrolę	Plėtoti kūrybiškumą ir rinkos poreikius atitit. KS įgūdžius	Gerinti viešojo ir SME KS brandą	Stiprinti tapt. KS pajėgumus ir gebėjimus
Skatinti nacionalinių pratybų vykdymą ir dalyvavimą tarp.		Skatinti viešojo ir privat. sektor. bei mokslo bendrad.	Kurti atsakingą IRT saugum. spragų atskleidimo praktiką	Plėtoti dialogą su JAV KS srityje
Plėtoti valstybės kibernet. gynybos pajėgumus				

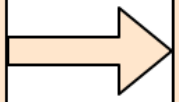
LIETUVOS KIBERNETINIO SAUGUMO TEISINĖ SISTEMA (buvo koreguojama)

Kai kurios sąvokos Kibernetinio saugumo įstatyme

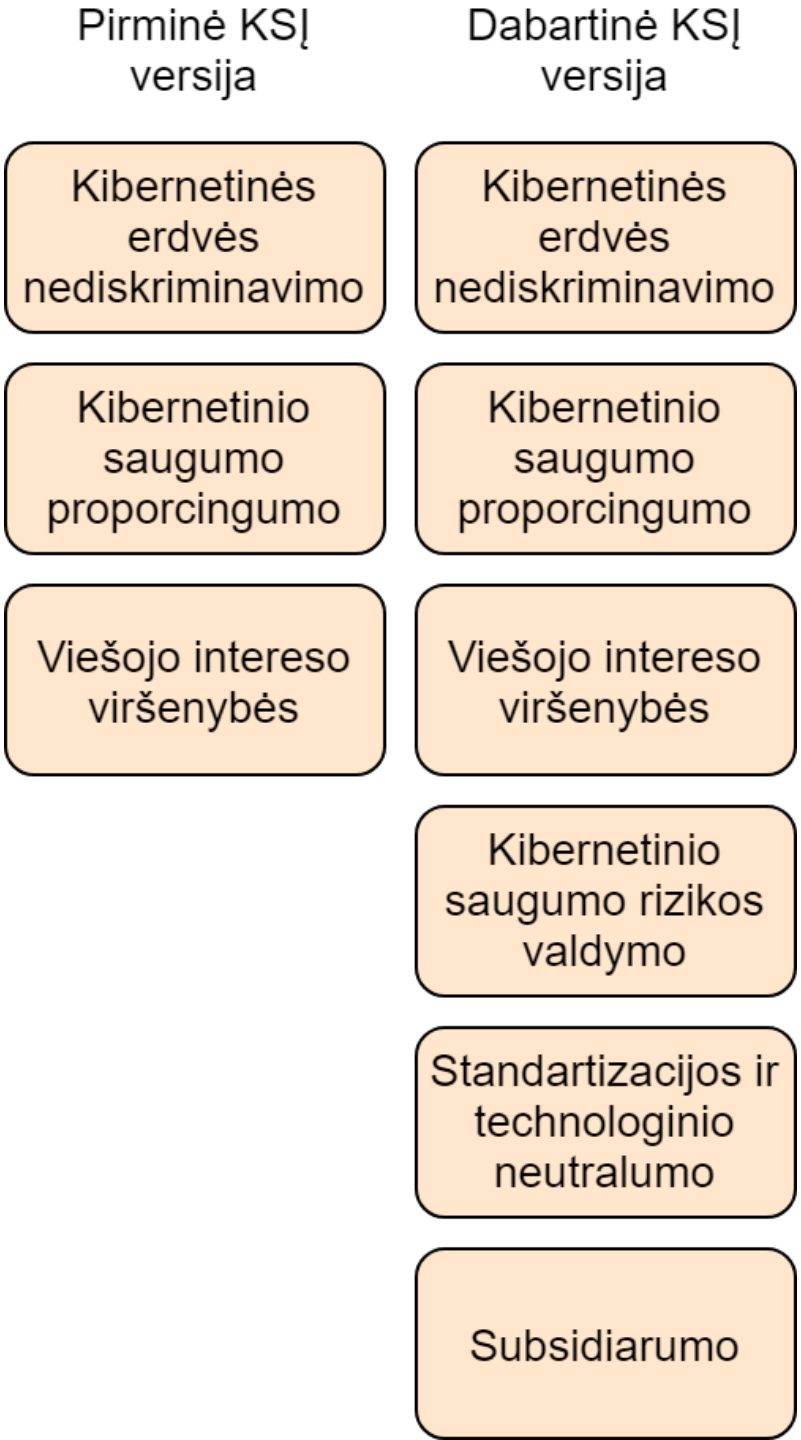
- **Kibernetinio saugumo subjektas** - subjektas, valdantis ir (arba) tvarkantis valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjas.
- **Elektroninės prekyvietės paslauga** - paslauga, kuria sudaromos sąlygos vartotojams ir (arba) komercinės veiklos subjektams sudaryti elektroninės prekybos ar paslaugų sutartis su komercinės veiklos subjektais elektroninės prekyvietės svetainėje arba komercinės veiklos subjekto svetainėje, kurioje naudojamasi elektroninės prekyvietės teikiamomis kompiuterijos paslaugomis.
- **Elektroninės informacijos prieglobos paslaugos** – paslaugos, apimančios galimybės naudotis elektroninės informacijos ir elektroninių duomenų (toliau – elektroninė informacija) kūrimo ir tvarkymo priemonėmis sudarymą ir (arba) paslaugų gavėjo pateiktos elektroninės informacijos laikymą.
- **Debesijos paslaugos** – paslaugos, kurių gavėjai nuotoliniu būdu naudojasi šių paslaugų teikėjų valdoma ryšių ir informacinių sistemų infrastruktūra.
- **Ypatingos svarbos informacinė infrastruktūra** – ryšių ir informacinė sistema ar jos dalis, ryšių ir informacinių sistemų grupė, kurioje įvykęs kibernetinis incidentas gali padaryti didelį neigiamą poveikį nacionaliniam saugumui, valstybės ūkiui, valstybės ir visuomenės interesams.

- **Kibernetinio saugumo krizė** - kibernetinis incidentas arba incidentai, kurių sukelto neigiamo poveikio Lietuvos Respublika negali pašalinti viena pati arba kurie Lietuvos Respublikai ir kitoms valstybėms, priklausančioms tarptautinėms organizacijoms, kurių narė yra Lietuvos Respublika, arba tų tarptautinių organizacijų institucijoms sukelia tokio masto ir tokios techninės arba politinės reikšmės neigiamą poveikį, kad iškyla poreikis koordinuoti politiką ir reaguoti tarptautiniu lygmeniu
- **Kibernetinis saugumas** – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą.
- **Kibernetinių incidentų valdymas** - procedūros, kurių tikslas – aptikti, analizuoti kibernetinius incidentus ir reaguoti į juos, taip pat atkurti įprastinę ryšių ir informacinių sistemų veiklą.
- **Ryšių ir informacinė sistema** - elektroninių ryšių tinklas, informacinė sistema, registras, pramoninių procesų valdymo sistema ir jų valdymo, naudojimo, apsaugos ir priežiūros tikslais laikoma, tvarkoma, atkuriama arba perduodama elektroninė informacija.
- **Skaitmeninės paslaugos** – ryšių ir informacinėmis technologijomis grindžiama paslaugų grupė, apimanti elektroninės prekyvietės, paieškos internete ir (arba) debesijos paslaugas.
- **Rizika** - pagrįstai nustatoma aplinkybė ar įvykis, galintis turėti neigiamą poveikį ryšių ir informacinių sistemų saugumui.

Kibernetinis incidentas– įvykis ar veika kibernetinėje erdvėje, sudarantys ar galintys sudaryti galimybę ar sąlygas neteisėtai prisijungti prie informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos, sutrikdyti ar pakeisti, įskaitant valdymo perėmimą, informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, taip pat sudaryti sąlygas pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją tokios teisės neturintiems asmenims.

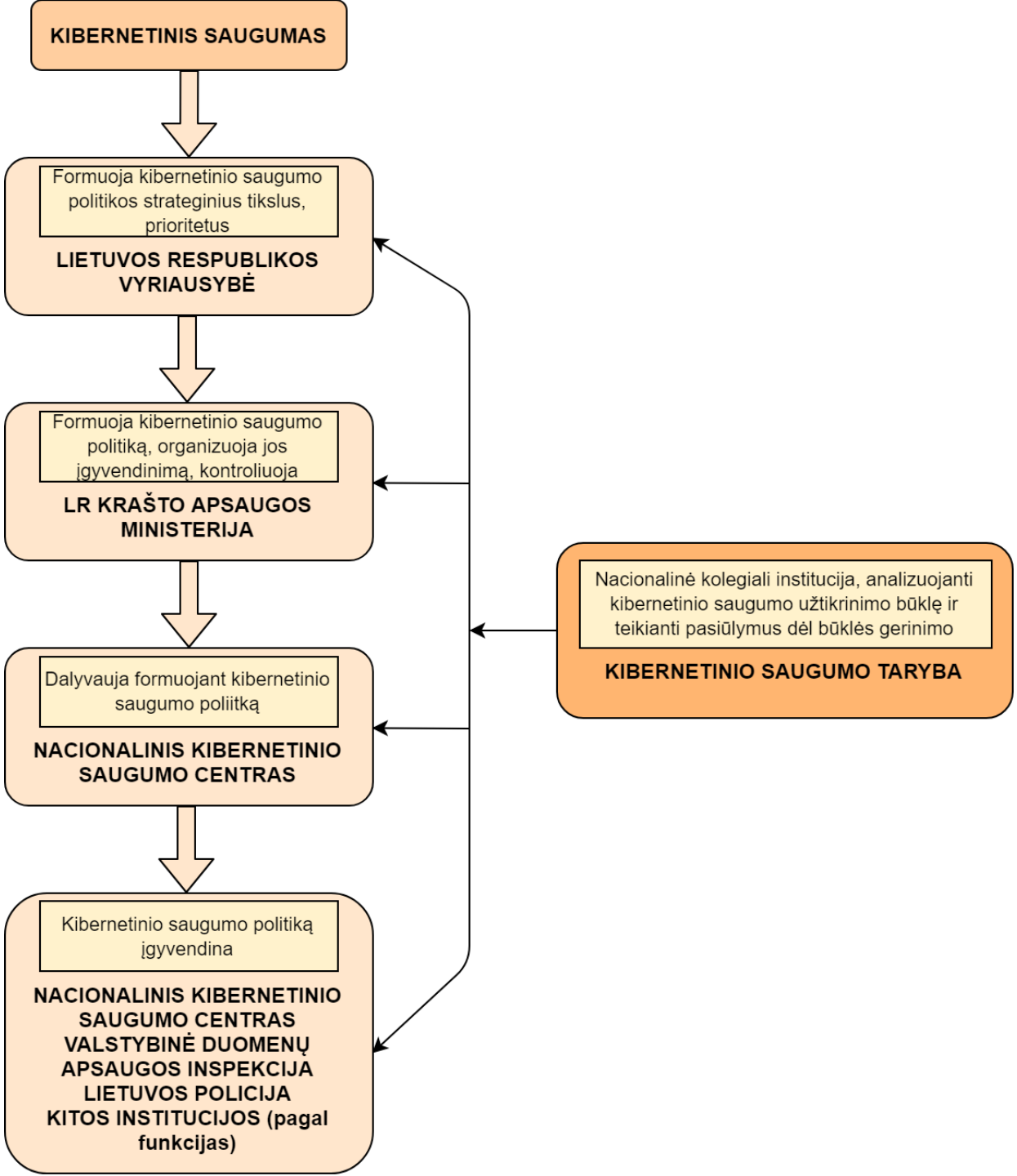


Kibernetinis incidentas–įvykis ar veika kibernetinėje erdvėje, galintys sukelti arba sukeliantys grėsmę arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintys trikdyti arba trikdantys ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą.

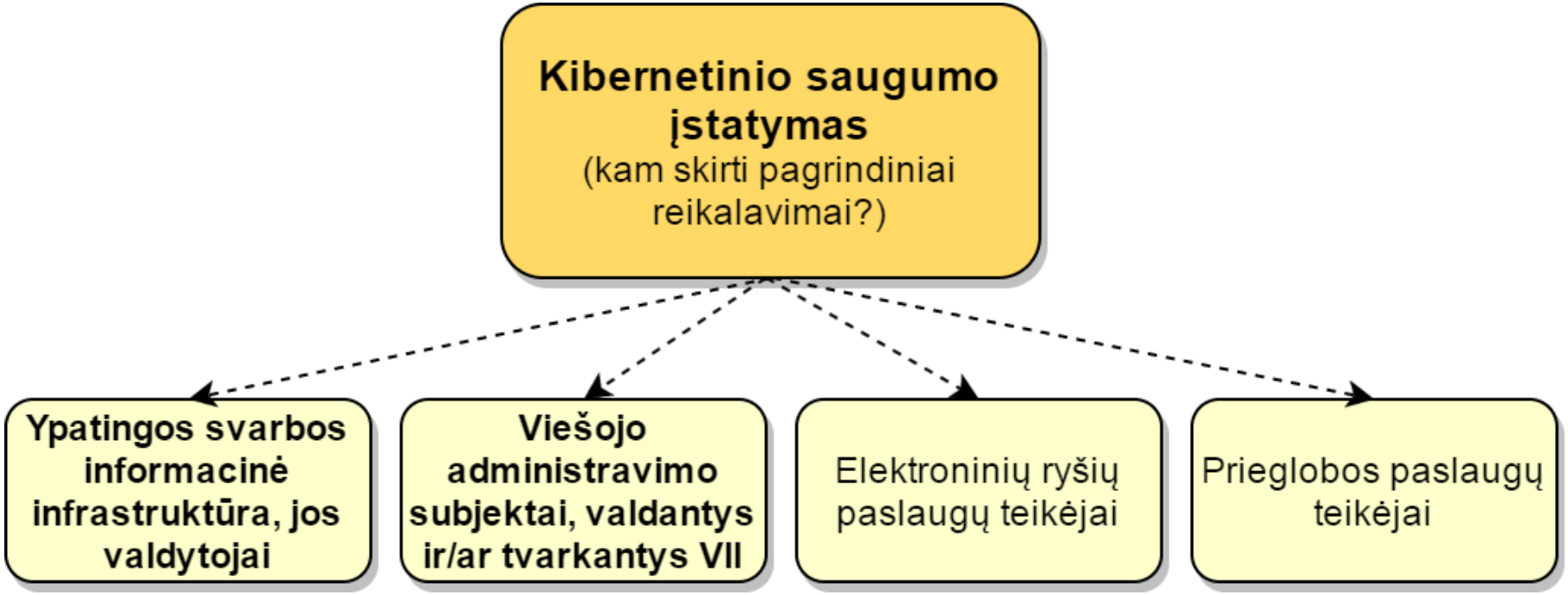


Kibernetinio saugumo principai pagal KSĮ

Atsakingo atskleidimo („**reponsible disclosure**“) principas?


KIBERNETINIS SAUGUMAS
Formuoja kibernetinio saugumo politikos strateginius tikslus, prioritetus
LIETUVOS RESPUBLIKOS VYRIAUSYBĖ
Formuoja kibernetinio saugumo politiką, organizuoja jos įgyvendinimą, kontroliuoja
LR KRAŠTO APSAUGOS MINISTERIJA
Dalyvauja formuojant kibernetinio saugumo poliitką
NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS
Kibernetinio saugumo politiką įgyvendina
NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS
VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA
LIETUVOS POLICIJA
KITOS INSTITUCIJOS (pagal funkcijas)
Nacionalinė kolegiali institucija, analizuojanti kibernetinio saugumo užtikrinimo būklę ir teikianti pasiūlymus dėl būklės gerinimo
KIBERNETINIO SAUGUMO TARYBA

Pradinis variantas



Valstybės informacinių išteklių rūšis	**Aprašymas**
Ypatingos svarbos valstybės informaciniai ištekliai	Juos sudaro visai valstybei svarbi informacija, apdorojama valstybės informacinėse sistemose ir pagrindiniuose valstybės registruose, ir ją apdorojančios valstybės informacinės sistemos ir pagrindiniai valstybės registrai
Svarbūs valstybės informaciniai ištekliai	Juos sudaro kelioms institucijoms svarbi informacija, apdorojama valstybės informacinėse sistemose ir valstybės registruose, ir ją apdorojančios valstybės informacinės sistemos ir valstybės registrai
Žinybinės svarbos valstybės informaciniai ištekliai	Juos sudaro vienai institucijai svarbi informacija, apdorojama valstybės informacinėse sistemose ir žinybiniuose registruose, ir ją apdorojančios valstybės informacinės sistemos ir žinybiniai registrai
Kiti valstybės informaciniai ištekliai	Juos sudaro informacija, kurią valdo institucija, atlikdama vidaus administravimo funkcijas, apdorojama kitomis informacinėse sistemose ir šią informaciją apdorojančios informacinės sistemos.

Valstybės informacinių išteklių svarbos **kategorijos nustatomos vadovaujantis** Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“.

TIS direktyva

Esminių paslaugų operatoriai

Operatorių identifikavimas
(trys požymiai, iš jų - didelis trikdomasis poveikis (klientų skaičius, rinkos dalis, geografinė teritorija ir kt.)).

Saugumo reikalavimai
Proporcingos techninės-organizacinėms priemonės, atitinkančios riziką.
Priemonės skirtos išvengti poveikio ir jį sumažinti, siekiant užtikrinti tęstinumą.

Pareiga be nepagrįsto delsimo **pranešti** apie incidentą, kuris turi didelį poveikį esminių paslaugų **tęstinumui**
- naudotojų skaičius,
- incidento trukmė,
- geografinė aprėptis.

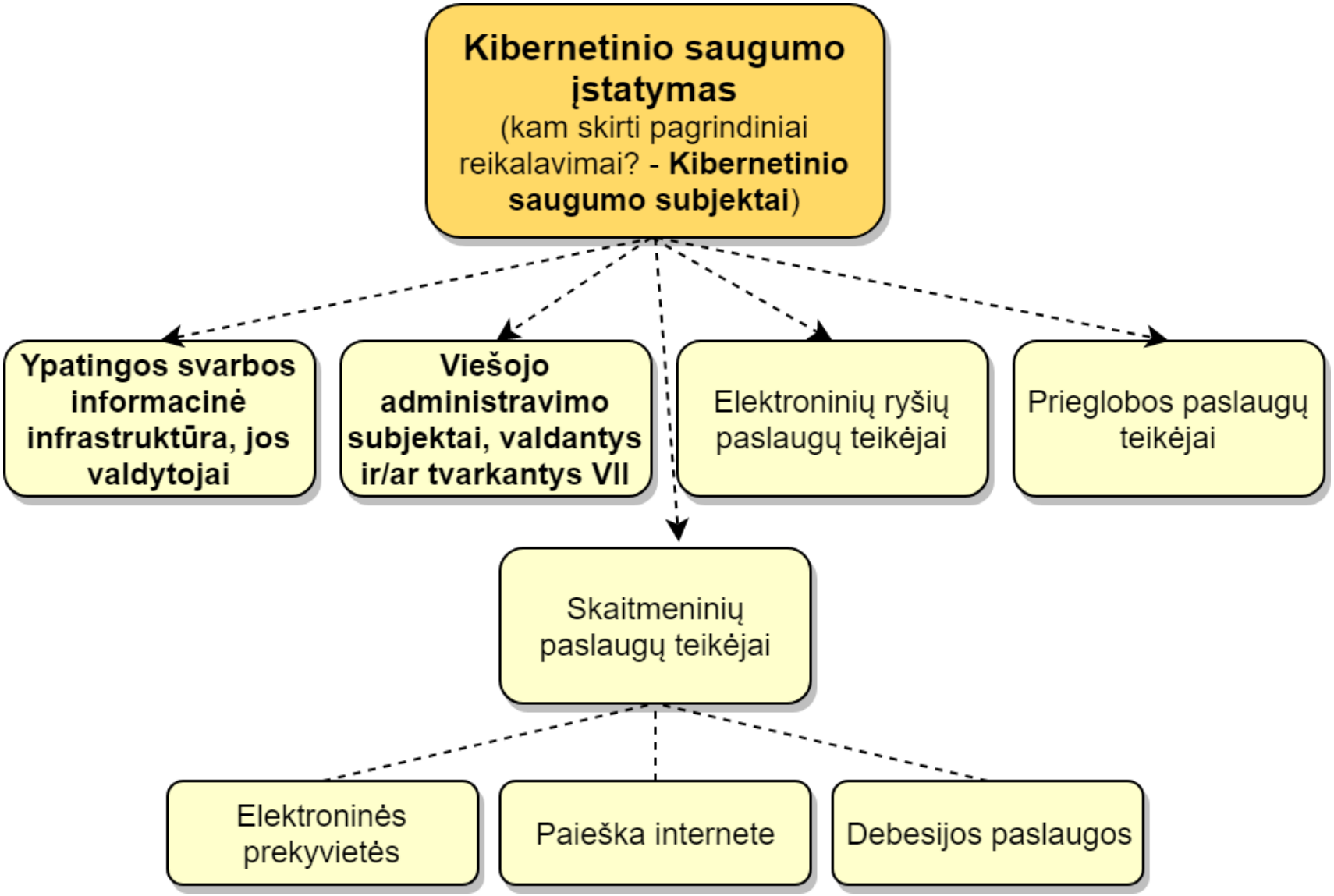
Skaitmeninių paslaugų teikėjai

Taikoma, jei atitinka IVP požymius:
1) e-prekyvietė,
2) interneto paieškos sistema,
3) debesų kompiuterijos paslauga.

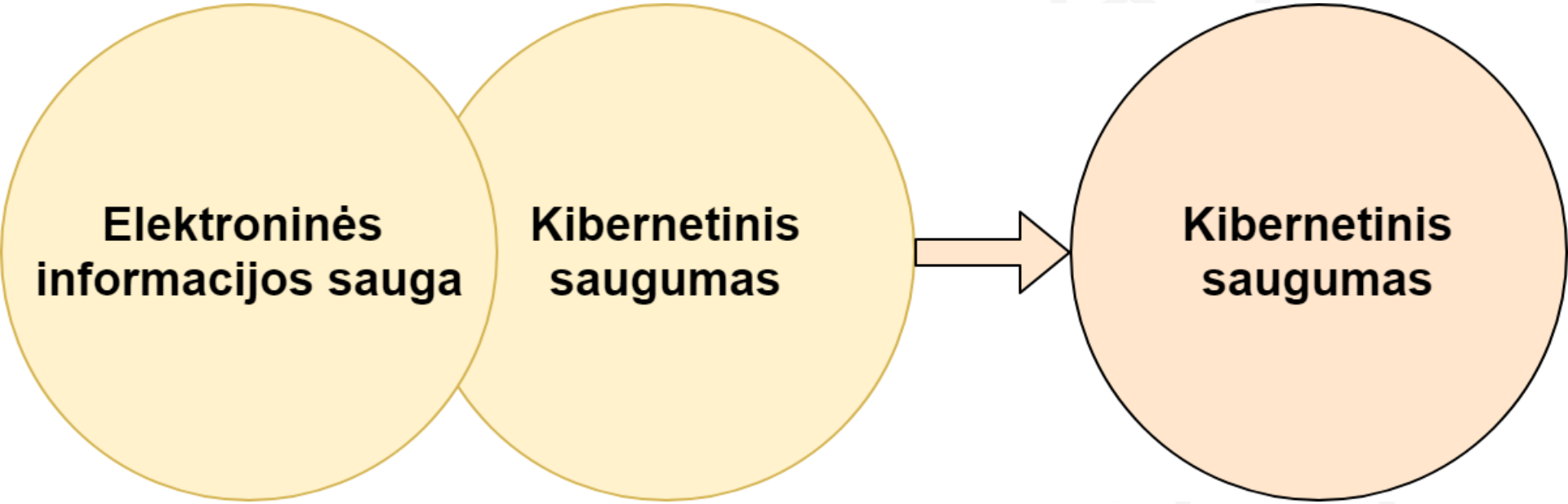
Saugumo reikalavimai*
Saugumo lygis turi atitikti atsiradusią riziką.
Atsižvelgiama į šiuos elementus:
- sistemų ir įrenginių saugumas;
- incidentų valdymas;
- veiklos tęstinumo valdymas ir kt.
**netaikomi mikro ir mažoms įmonėms, t.y. iki 250 darbuot. ir ne daugiau 50 mln. apyvartos.*

Pareiga be nepagrįsto delsimo **pranešti** apie incidentą, kuris turi didelį poveikį paslaugos **teikimui**
- naudotojų skaičius,
- incidento trukmė,
- geografinė aprėptis,
- sutrikdymo mastas,
- poveikio ekonominei/visuomeninei veiklai mastas.

Tapo po pakeitimų



Kibernetinio saugumo reguliavimo tendencijos



NKSC. NKSC FUNKCIJOS (KSI 8 str.):

1) Atlieka kibernetinio saugumo subjektų ir jų valdomų RIS atitikties org.-tech. reikalavimams **priežiūrą** ir saugumo būklės tyrimus.
2) Duoda **nurodymus** pateikti informaciją atitikties būklei įvertinti.
3) Taiko technines priemones VII ir YSII atsparumui įvertinti.
4) Duoda **nurodymus** dėl saugumo užtikrinimo ir trūkumų pašalinimo.
5) Duoda **nurodymus** atlikti RIS auditą (išskyrus skaitmeninių pasl. teikėjus).
6) (*gavus informaciją*) Duoda nurodymus skaitmeninų paslaugų teikėjams.
7) Nacionaliniu lygiu stebi kibernetinius incidentus, atlieka rizikos, incidentų analizę.
8) Diegia ir valdo technines saugumo priemones VII bei YSII.
9) Nacionaliniu lygiu organizuoja kibernetinių incidentų valdymą.
10) Kibernetinio incidento metu taiko būtinas saugumo priemones.
11) Siekdamas sustabdyti kibernetinio incidento poveikį VII ar YSII, duoda nurodymus ER paslaugų teikėjams.
12) Dalyvauja kibernetinio saugumo krizių valdyme.
13) Informuoja visuomenę apie pavienius incidentus arba reikalauja, kad tai padarytų kibernetinio saugumo subjektas.
14) Bendradarbiauja su kompetentingomis institucijomis, turi teisę jas pasitelkti.
15) Tvarko asmens duomenis, būtinus NKSC funkcijoms atlikti, ADTAĮ tvarka.
16) Plėtoja kibernetinį saugumą stiprinančius projektus.

KIBERNETINIO SAUGUMO SUBJEKTŲ PAREIGOS PAGAL KIBERNETINIO SAUGUMO ĮSTATYMĄ

Bendrosios kibernetinio saugumo subjektų pareigos

Specialiosios kibernetinio saugumo subjektų pareigos

Pastaba: pagal KSĮ, SPT atveju, netaikoma mažoms ir labai mažoms įmonėms!

Dėl mažų ir labai mažų įmonių - Smulkiojo ir vidutinio verslo plėtros įstatymas.
2. **Maža įmonė** – įmonė, kurioje dirba mažiau kaip **50 darbuotojų** ir kurios finansiniai duomenys atitinka bent vieną iš šių sąlygų:
1) įmonės metinės pajamos **neviršija 10 mln. eurų**;
2) įmonės **balanse nurodyto turto vertė neviršija 10 mln. eurų**.
3. **Labai maža įmonė** – įmonė, kurioje dirba mažiau kaip 10 darbuotojų ir kurios finansiniai duomenys atitinka bent vieną iš šių sąlygų:
1) įmonės metinės pajamos neviršija 2 mln. eurų;
2) įmonės balanse nurodyto turto vertė neviršija 2 mln. eurų.

Kibernetinio saugumo subjektų (bendrosios) pareigos pagal KSĮ

1) **atsako už** jų valdomų ryšių ir informacinių sistemų ar teikiamų paslaugų kibernetinį saugumą, **užtikrina** jų **atitiktį** organizaciniams ir techniniams kibernetinio saugumo **reikalavimams**, taikomiems kibernetinio saugumo subjektams;

2) organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše nustatyta tvarka **atlieka rizikos vertinimą ir įdiegia kitas**, naujausiais technikos laimėjimais paremtas ir nustatytai rizikai proporcingas, technines ir organizacines kibernetinio saugumo **priemones**;

3) Nacionaliniame kibernetinių incidentų valdymo plane nustatytomis sąlygomis ir tvarka **praneša Nacionaliniam kibernetinio saugumo centrui** apie jų valdomose ir (arba) tvarkomose ryšių ir informacinėse sistemose įvykusius kibernetinius **incidentus** ir taikytas kibernetinių incidentų valdymo priemones;

4) policijos generalinio komisaro nustatyta tvarka **teikia policijai informaciją**, reikalingą teisės pažeidimams, turintiems nusikalstamų veikų požymių, kibernetinėje erdvėje užkardyti ir tirti, ir vykdo kitus policijos nurodymus, duotus šio įstatymo nustatytais pagrindais. Policijos nurodymus dėl paslaugų teikimo jų gavėjui apribojimo privaloma įvykdyti ne vėliau kaip per 8 valandas nuo policijos nurodymo gavimo;

5) **paskiria kompetentingą asmenį ar padalinį**, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą, ir Nacionaliniam kibernetinio saugumo centrui pateikia šio asmens ar padalinio kontaktinę informaciją;

6) **vykdo** šio įstatymo 8 straipsnyje nustatytus Nacionalinio kibernetinio saugumo **centro nurodymus**.

Bendrosios kibernetinio saugumo subjektų pareigos

Specialiosios kibernetinio saugumo subjektų pareigos

YSII valdytojai:
- tvirtina ir NKSC pateikia KI valdymo planus;
- praneša skaitmeninių paslaugų teikėjams apie neigiamą poveikį YSII;
- ne rečiau kaip kartą per metus išbando KI valdymo planuose numatytų priemonių veikimą ir rezultatus pateikia NKSC;
- sudaro sąlygas NKSC diegti, valdyti ir taikyti technines priemones (siekiant įvertinti atsparumą).

Subjektai, valdantys VII:
- sudaro sąlygas NKSC diegti, valdyti ir taikyti technines priemones (siekiant įvertinti atsparumą).

ER paslaugų teikėjai / El. informacijos prieglobos paslaugų teikėjai:
- viešai skelbia rekomendacijas kibernetiniam saugumui užtikrinti.

Skaitmeninių paslaugų teikėjai:
- viešai skelbia rekomendacijas kibernetiniam saugumui užtikrinti.
- skiria atstovą ES.

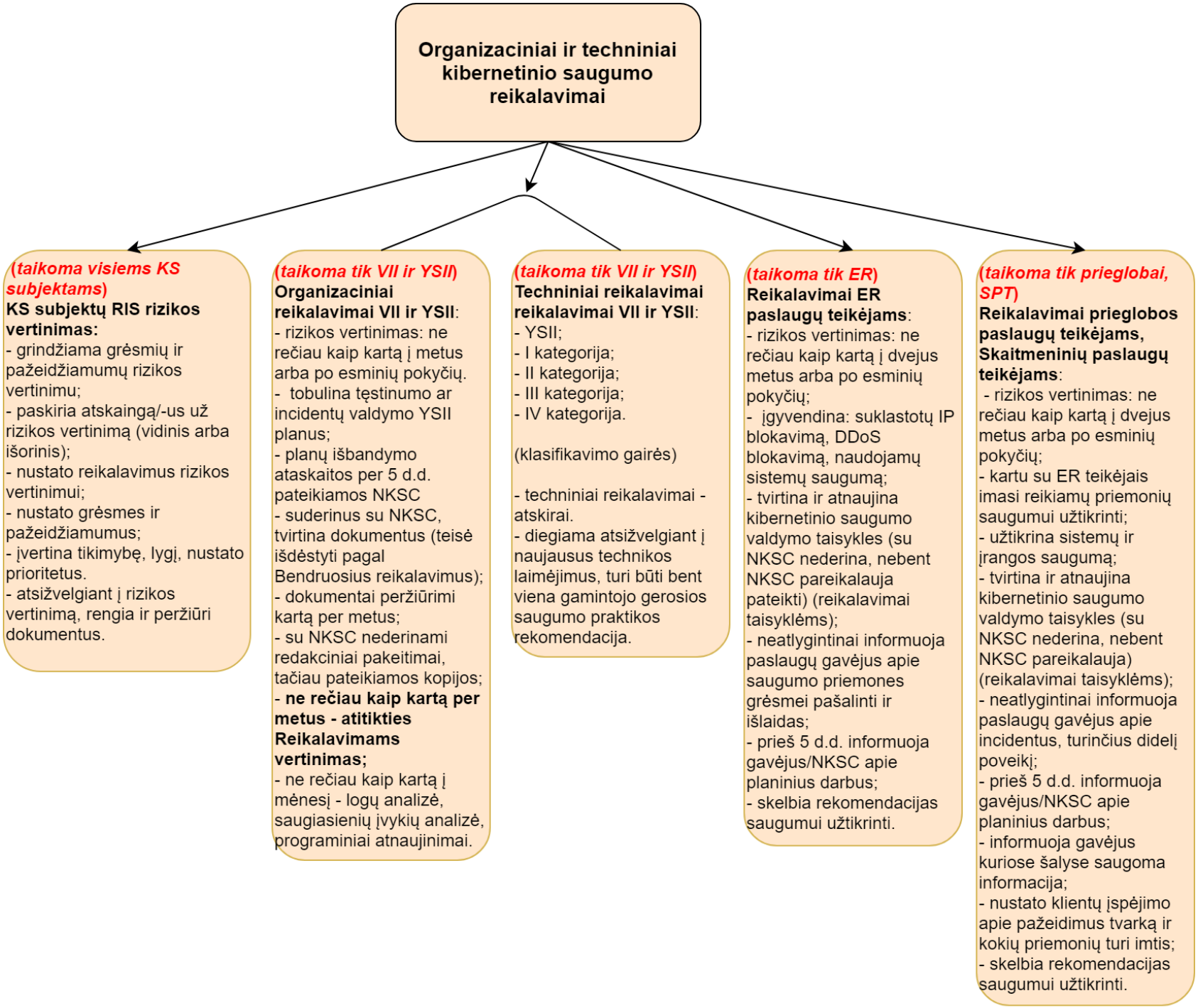
ORGANIZACINIAI IR TECHNINIAI KIBERNETINIO SAUGUMO REIKALAVIMAI

2020 m. lapkričio 18 d. pakeitimai:

„13[1]. Ypatingos svarbos informacinės infrastruktūros valdytojai Apraše nustatytus **organizacinius** kibernetinio saugumo reikalavimus privalo įgyvendinti ne vėliau kaip **per 12 mėnesių** nuo jų įtraukimo į Lietuvos Respublikos Vyriausybės patvirtintą ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašą.“

1.4.2. Papildyti 17[1] punktu:

„17[1]. Ypatingos svarbos informacinės infrastruktūros valdytojai Apraše nustatytus **techninius** kibernetinio saugumo reikalavimus privalo įgyvendinti ne vėliau kaip **per 24 mėnesius** nuo jų įtraukimo į Lietuvos Respublikos Vyriausybės patvirtintą ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašą.“


Organizaciniai ir techniniai kibernetinio saugumo reikalavimai
(taikoma visiems KS subjektams)
KS subjektų RIS rizikos vertinimas:
- grindžiama grėsmių ir pažeidžiamumų rizikos vertinimu;
- paskiria atskaingą/-us už rizikos vertinimą (vidinis arba išorinis);
- nustato reikalavimus rizikos vertinimui;
- nustato grėsmes ir pažeidžiamumus;
- įvertina tikimybę, lygį, nustato prioritetus.
- atsižvelgiant į rizikos vertinimą, rengia ir peržiūri dokumentus.
(taikoma tik VII ir YSII)
Organizaciniai reikalavimai VII ir YSII:
- rizikos vertinimas: ne rečiau kaip kartą į metus arba po esminių pokyčių.
- tobulina tęstinumo ar incidentų valdymo YSII planus;
- planų išbandymo ataskaitos per 5 d.d. pateikiamos NKSC
- suderinus su NKSC, tvirtina dokumentus (teisė išdėstyti pagal Bendruosius reikalavimus);
- dokumentai peržiūrimi kartą per metus;
- su NKSC nederinami redakciniai pakeitimai, tačiau pateikiamos kopijos;
- ne rečiau kaip kartą per metus - atitikties Reikalavimams vertinimas;
- ne rečiau kaip kartą į mėnesį - logų analizė, saugiasienių įvykių analizė, programiniai atnaujinimai.
(taikoma tik VII ir YSII)
Techniniai reikalavimai VII ir YSII:
- YSII;
- I kategorija;
- II kategorija;
- III kategorija;
- IV kategorija.
(klasifikavimo gairės)
- techniniai reikalavimai - atskirai.
- diegiama atsižvelgiant į naujausus technikos laimėjimus, turi būti bent viena gamintojo gerosios saugumo praktikos rekomendacija.
(taikoma tik ER)
Reikalavimai ER paslaugų teikėjams:
- rizikos vertinimas: ne rečiau kaip kartą į dvejus metus arba po esminių pokyčių;
- įgyvendina: suklastotų IP blokavimą, DDoS blokavimą, naudojamų sistemų saugumą;
- tvirtina ir atnaujina kibernetinio saugumo valdymo taisykles (su NKSC nederina, nebent NKSC pareikalauja pateikti) (reikalavimai taisyklėms);
- neatlygintinai informuoja paslaugų gavėjus apie saugumo priemones grėsmei pašalinti ir išlaidas;
- prieš 5 d.d. informuoja gavėjus/NKSC apie planinius darbus;
- skelbia rekomendacijas saugumui užtikrinti.
(taikoma tik prieglobai, SPT)
Reikalavimai prieglobos paslaugų teikėjams, Skaitmeninių paslaugų teikėjams:
- rizikos vertinimas: ne rečiau kaip kartą į dvejus metus arba po esminių pokyčių;
- kartu su ER teikėjais imasi reikiamų priemonių saugumui užtikrinti;
- užtikrina sistemų ir įrangos saugumą;
- tvirtina ir atnaujina kibernetinio saugumo valdymo taisykles (su NKSC nederina, nebent NKSC pareikalauja) (reikalavimai taisyklėms);
- neatlygintinai informuoja paslaugų gavėjus apie incidentus, turinčius didelį poveikį;
- prieš 5 d.d. informuoja gavėjus/NKSC apie planinius darbus;
- informuoja gavėjus kuriose šalyse saugoma informacija;
- nustato klientų įspėjimo apie pažeidimus tvarką ir kokių priemonių turi imtis;
- skelbia rekomendacijas saugumui užtikrinti.

e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr

Pradžia | Paieška | Vertinimų vidurkis: 5 | LT

Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo

Rūšis:	Nutarimas
Identifikacinis kodas:	2018-13252
Užregistravimo TAR data:	2018-08-21
Galioja	Įsigalioja 2018-08-22
Kalba:	Lietuvių

Priėmimo data:	2018-08-13
Dokumento nr.:	818
Priėmė:	Lietuvos Respublikos Vyriausybė
Paskelbta:	TAR, 2018-08-21, Nr. 13252

Galiojanti suvestinė redakcija:	2019-04-27 -
Suvestinių redakcijų sąrašas pagal datą:	
Pakeitimų projektai:	Nėra
Eurovoc terminai:	
Ryšys su ES teisės aktais:	Nėra

Galiojanti suvestinė redakcija (nuo 2019-04-27)

Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo priedas

TECHNINIŲ KIBERNETINIO SAUGUMO REIKALAVIMŲ, TAIKOMŲ SUBJEKTAMS, VALDANTIEMS IR (ARBA) TVARKANTIEMS VALSTYBĖS INFORMACINIUS IŠTEKLIUS, YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS VALDYTOJAMS, SĄRAŠAS

1 lentelė. Atpažinties, tapatumo patvirtinimo ir naudojimosi valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra saugumas ir kontrolė

Reikalavimas	Kategorija pagal svarbą				
	Ypatingos svarbos informacinė infrastruk-tūra (YSII)	I	II	III	IV
1. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros priežiūrą vykdančio asmens (toliau – administratorius) funkcijos turi būti atliekamos naudojant atskirą tam skirtą paskyrą, kuri negali būti naudojama kasdienėms valstybės informacinių išteklių ar ypatingos svarbos	x	x	x	x	x
5. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojas ar administratorius turi patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone	x	x	x	x	x
6. Administratorių tapatumui patvirtinti turi būti naudojamos dviejų veiksnių tapatumo patvirtinimo priemonės (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	x	x		
7. Valstybės informacinių	x	x	x	x	x

Susijusi informacija

- Teisės akto pakeitimai (2)
- Susiję dokumentai (5)

Techniniai reikalavimai

- Atpažinties, tapatumo patvirtinimo ir naudojimosi saugumas ir kontrolė
- Naudotojų ir administratorių atliekamų veiksmų auditas ir kontrolė
- Įsibrovimų aptikimas ir prevencija
- Belaidžio tinklo saugumas ir kontrolė
- Mobiliųjų įrenginių (prijungtų prie RIS) saugumas ir kontrolė
- Naudojamos svetainės saugumas ir kontrolė
- Naudojamo interneto saugumas ir kontrolė

Kiti organizacinių ir techninių kibernetinio saugumo reikalavimų aspektai

- Kibernetinio saugumo subjektai **gali taikyti papildomus reikalavimus**. Jei saugumo priemonės yra lygiavertės ir apima Apraše nustatytus reikalavimus, kibernetinio saugumo subjektai gali taikyti tik papildomus reikalavimus.
- Kibernetinio saugumo subjektai, išskyrus SPT, teikia NKSC techninę informaciją, reikalingą RIS saugumui įvertinti (NKSC reikalavimu ar savo iniciatyva).
- Diegiant technines saugumo priemones **ER, prieglobos ir SPT, rekomenduotina** vadovautis techninių kibernetinio saugumo reikalavimų sąrašu.
- Perkant darbus ir (ar) įrangą, susijusią su VII ar KI – pirkimo sąlygose nustatyti, kad **paslaugų teikėjas ir (ar) įrangos tiekėjas užtikrina atitiktį Reikalavimams** (žr. Reikalavimų 13 p.).
- Praktinė problema – visų klausimų delegavimas IT specialistams.
- **REGULIAVIMO TENDENCIJOS**: artimiausiu metu turėtų būti paskelbtas projektas dėl kibernetinio saugumo reikalavimų nustatymo! Esmė – org.-tech. reikalavimai, diferencijuoti pagal rizikos lygį.

Problemos viešajame sektoriuje

Dažniausios problemos:

- Formali atitiktis kibernetiniame saugume;
- Kibernetinio saugumo rizikos vertinamos paviršutiniškai (*RC atvejis: rizika buvo numatyta, tačiau valdant incidentą kilo problemų*);
- Interneto svetainių saugumas – nemaža dalis svetainių nėra saugios.
- Kibernetinio saugumo kultūra, kibernetinio saugumo higiena;
- Kibernetinio saugumo mokymų buvimas ir efektyvumas (kokybė);
- Vadovybės supratimo svarba;
- Už kibernetinį saugumą atsakingo asmens / padalinio turėjimas.
- Perkėlimo į could tendencijos.

Administracinių nusižengimų kodeksas

479 straipsnis. Lietuvos Respublikos kibernetinio saugumo įstatymo nuostatų dėl pareigos teikti informaciją pažeidimai

1. Informacijos apie kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones nepateikimas Nacionaliniam kibernetinio saugumo centrui arba šios informacijos teikimo tvarkos pažeidimas

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.

2. Nacionalinio kibernetinio saugumo centro nurodymų kibernetinio saugumo subjektams pateikti informaciją, būtiną kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams, taikomiems kibernetinio saugumo subjektams, ir kibernetinio saugumo būklei įvertinti, nevykdymas laiku

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.

3. Informacijos apie kibernetinius incidentus, galimai turinčius nusikalstamų veikų požymių, nepateikimas policijai arba šios informacijos teikimo tvarkos pažeidimas

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki trijų šimtų eurų.

4. Šio straipsnio 1, 2, 3 dalyse numatyti administraciniai nusižengimai, padaryti pakartotinai,

užtraukia baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trijų šimtų iki vieno tūkstančio keturių šimtų keturiasdešimt eurų.

Straipsnio pakeitimai:

Nr. XIII-922, 2017-12-19, paskelbta TAR 2017-12-29, i. k. 2017-21594

Nr. XIII-1427, 2018-06-30, paskelbta TAR 2018-07-11, i. k. 2018-11734

480 straipsnis. Lietuvos Respublikos kibernetinio saugumo įstatyme nustatytų kibernetinio saugumo užtikrinimo pareigų atlikimo pažeidimai

Pakeistas straipsnio pavadinimas:
Nr. XIII-1427, 2018-06-30, paskelbta TAR 2018-07-11, i. k. 2018-11734

1. Teisėtų Nacionalinio kibernetinio saugumo centro ar policijos nurodymų, susijusių su kibernetinio saugumo užtikrinimu, neįvykdymas laiku

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo septyniasdešimt iki vieno šimto penkiasdešimt eurų.

Straipsnio dalies pakeitimai:
Nr. XIII-922, 2017-12-19, paskelbta TAR 2017-12-29, i. k. 2017-21594
Nr. XIII-1427, 2018-06-30, paskelbta TAR 2018-07-11, i. k. 2018-11734

2. Šio straipsnio 1 dalyje numatytas administracinis nusižengimas, padarytas pakartotinai,

užtraukia baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trijų šimtų iki penkių šimtų septyniasdešimt eurų.

3. Kibernetinių incidentų valdymo ypatingos svarbos informacinėje infrastruktūroje plano neparengimas ar nepatvirtinimas arba nepateikimas Nacionaliniam kibernetinio saugumo centrui

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki vieno tūkstančio keturių šimtų eurų.

4. Nustatytų organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų kibernetiniam saugumui užtikrinti nevykdymas

užtraukia įspėjimą arba baudą juridinių asmenų vadovams ar kitiems atsakingiems asmenims nuo trisdešimt iki vieno tūkstančio keturių šimtų eurų.

Straipsnio dalies pakeitimai:
Nr. XIII-922, 2017-12-19, paskelbta TAR 2017-12-29, i. k. 2017-21594
Nr. XIII-1427, 2018-06-30, paskelbta TAR 2018-07-11, i. k. 2018-11734

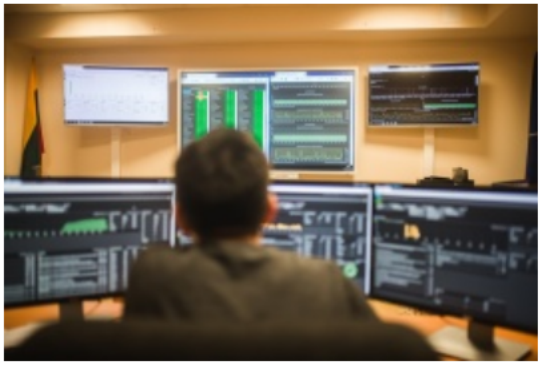
5. Šio straipsnio 3, 4 dalyse numatyti administraciniai nusižengimai, padaryti pakartotinai,

užtraukia baudą juridinių asmenų vadovams ar kitiems asmenims nuo vieno tūkstančio keturių šimtų iki penkių tūkstančių aštuonių šimtų eurų.

Atsakingo atskleidimo (angl. *responsible disclosure*) reguliavimas – 2021 m. Kibernetinio saugumo įstatymo pakeitimai

LR Seimas įteisino atsakingą kibernetinių spragų atskleidimą

2021.06.17



Birželio 17 d. LR Seimas patvirtino Kibernetinio saugumo įstatymo pataisas, kurios įteisino atsakingo ryšių ir informacinių sistemų spragų atskleidimo procesą. Pataisos įsigalios, kai jas pasirašys LR Prezidentas.

„Dauguma ryšių ir informacinių sistemų turi didesnių ar mažesnių spragų. Nustatę aiškias sąlygas, kada galima teisėtai jų ieškoti ir kaip tinkamai apie jas pranešti, mes ne tik užkirsime kelią būsimiems kibernetiniams incidentams, bet ir stiprinsime bendrą mūsų šalies kibernetinę brandą“, – sako krašto apsaugos ministras Arvydas Anušauskas.

Ryšių ir informacinių sistemų spraga – tai ryšių ir informacinės sistemos trūkumas, dėl kurio gali įvykti kibernetinis incidentas.

Spragų atskleidimas yra laikomas atsakingu, kai informacija apie aptiktas spragas yra, visų pirma, pateikiama pačiai organizacijai, kurios sistemose ar produktuose jos buvo aptiktos, ir/ar spragų atskleidimo procesą koordinuojančiai institucijai. Pagal Seimo patvirtintas Kibernetinio saugumo įstatymo pataisas, Lietuvoje šią koordinavimo funkciją vykdys Nacionalinis kibernetinio saugumo centras (NKSC) prie Krašto apsaugos ministerijos.

Spragų paieška ir jų atskleidimas yra laikomi teisėtais ir tokius veiksmus atlikusiam asmeniui neužtraukia teisinės atsakomybės, kai vykdant šią veiklą nėra trikdomas ryšių ir informacinės sistemos darbas, funkcionalumas, teikiamos paslaugos ir duomenų prieinamumas. Taip pat nesiekiama be reikalo, daugiau, negu reikia spragai patvirtinti, stebėti, fiksuoti, perimti, įgyti, laikyti, atskleisti, kopijuoti, keisti duomenų, nebandoma atspėti slaptažodžius, nenaudojami neteisėtu būdu gauti slaptažodžiai ir nėra manipuliuojama organizacijos darbuotojais.

e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr

Pradžia | Paieška | Vertinimų vidurkis: 3

Dokumento struktūra

V SKYRIUS
PRANEŠIMAI APIE SPRAGAS IR KIBERNETINIUS INCIDENTUS

Pakeistas skyriaus pavadinimas:
Nr. XIV-413, 2021-06-17, paskelbta TAR 2021-06-23, i. k. 2021-14159

16 straipsnis. Savanoriškas pranešimas apie kibernetinius incidentus

1. Asmenys, kuriems šiame įstatyme nėra nustatytos pareigos pranešti apie kibernetinius incidentus jų valdomose ryšių ir informacinėse sistemose, turi teisę savanoriškai pranešti Nacionaliniam kibernetinio saugumo centrui apie kibernetinius incidentus ir taikytas kibernetinių incidentų valdymo priemones. Nacionalinis kibernetinio saugumo centras tokius pranešimus tvarko Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka.

2. Asmeniui, savanoriškai pranešusiam apie kibernetinį incidentą, nenustatoma pareigų, susijusių su pranešimo pateikimu.

17 straipsnis. Spragų paieška ir atskleidimas

1. Spragų paieška ir atskleidimas laikomi teisėtais ir tokius veiksmus atlikusiam asmeniui neužtraukia teisinės atsakomybės tik tais atvejais, kai spragų paieška atliekama laikantis šio straipsnio 2 dalyje, nacionalinės spragų atskleidimo tvarkos apraše ir (ar) kibernetinio saugumo subjekto nustatytos spragų atskleidimo tvarkos apraše, taip pat šio straipsnio 5 dalyje numatytų apribojimų.

2. Atliekant spragų paiešką laikomasi šių apribojimų:

- Dauguma ryšių ir informacinių sistemų turi didesnių ar mažesnių spragų. Nustatytos aiškios sąlygos, kada galima teisėtai jų ieškoti ir kaip tinkamai apie jas pranešti. Tuo pačiu tai ir kibernetinio **saugumo incidentų prevencija**.
- Ryšių ir informacinių sistemų **spraga** – tai ryšių ir informacinės sistemos trūkumas, dėl kurio gali įvykti kibernetinis incidentas.
- **Spragų atskleidimas yra laikomas atsakingu**, kai informacija apie aptiktas spragas yra, visų pirma, pateikiama pačiai organizacijai, kurios sistemose ar produktuose jos buvo aptiktos, ir/ar spragų atskleidimo procesą koordinuojančiai institucijai - NKSC.
- Spragų paieška ir jų atskleidimas **yra laikomi teisėtais** ir tokius veiksmus atlikusiam asmeniui **neužtraukia teisinės atsakomybės**, **kai** vykdant šią veiklą nėra trikdomas ryšių ir informacinės sistemos darbas, funkcionalumas, prieinamumas. Taip pat nesiekiama be reikalo, daugiau, negu reikia spragai patvirtinti, stebėti, fiksuoti, perimti, įgyti, laikyti, atskleisti, kopijuoti, keisti duomenų, nebandoma atspėti slaptažodžius, nenaudojami neteisėtu būdu gauti slaptažodžiai ir nėra manipuliuojama organizacijos darbuotojais. Taip pat neturi būti dalinamasi informacija apie spragą.
- Asmuo, aptikęs spragą, turi nedelsiant **nutraukti** tolimesnę paiešką ir, ne vėliau kaip per 24 val., apie tai **pranešti** organizacijai, kurios sistemose ar produktuose ji buvo aptikta, ir/ar Nacionaliniam kibernetinio saugumo centrui jo interneto svetainėje užpildant specialią pranešimų formą arba informuojant el. paštu cert@nksc.lt.
- **KIBERNETINIO SAUGUMO SUBJEKTO NUSTATYTA SPRAGŲ ATSKLEIDIMO TVARKA**
- **90 dienų laikotarpis viešinimui.**
- Kibernetinio saugumo įstatymo pataisos numato prievolę **informuoti** ne tik apie aptiktas spragas, **bet ir apie vykdytą spragų paiešką**. Apie tokią veiklą asmuo privalo informuoti ne vėliau kaip per 24 val. nuo paieškos pradžios, o paiešką tęsiant ilgiau kaip parą – kas 24 val.
- Atskira **pranešimo forma NKSC**: https://www.nksc.lt/pranesti-spraga.html
- KAM ministras liepos 9 d. patvirtino ir **spragų paieškos tvarkos aprašą**: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/270e6bd1e08911eb866fe2e083228059

Viešųjų pirkimų įstatymo pakeitimai (2022)

e-seimas.lrs.lt/portal/legalAct/lt/TAD/0ed02bd3a5ff11ecaf79c2120caf5094?jfwid=-f3xm4jt50

Pradžia | Paieška | Vertinimų vidurkis: 0

Lietuvos Respublikos viešųjų pirkimų įstatymo Nr. I-1491 2, 17, 25, 27, 35, 37, 39, 45, 47, 51, 90 ir 92 straipsnių pakeitimo įstatymas

Rūšis:	Įstatymas
Identifikacinis kodas:	2022-05371
Užregistravimo TAR data:	2022-03-23
Neįsigaliojęs	Įsigalioja 2022-04-01 (Įstatymo 8, 10, 11 straipsniai,12 straipsnio 4 dalis ir 13 straipsnio 2, 4 dalys įsigalioja 2022-03-24)
Kalba:	Lietuvių

Priėmimo data:	2022-03-17
Dokumento nr.:	XIV-954
Priėmė:	Lietuvos Respublikos Seimas
Paskelbta:	TAR, 2022-03-23, Nr. 5371

Galiojanti suvestinė redakcija
Suvestinių redakcijų sąrašas pagal datą:
Pakeitimų projektai:
Eurovoc terminai:
Ryšys su ES teisės aktais:

Dokumento struktūra

Teisės akto tekstas (Nuorašas:)

3. Papildyti 37 straipsnį 9 dalimi:

„9. Perkančioji organizacija, veikianti gynybos srityje, valdanti ypatingos svarbos informacinę infrastruktūrą, veikianti srityse, kurios laikomos nacionaliniam saugumui užtikrinti strategiškai svarbių ūkio sektorių dalimi, ar įrašyta į Saugiojo tinklo naudotojų sąrašą, atlikdama prekių ir paslaugų pirkimus, kurių objektų BVPŽ kodai nurodomi šio įstatymo 92 straipsnio 13 dalyje numatytame sąraše, laiko, kad prekės ar paslaugos kelia grėsmę nacionaliniam saugumui, kai:

1) techninės ar programinės įrangos gamintojas ar jį kontroliuojantis asmuo yra registruoti (jeigu gamintojas ar jį kontroliuojantis asmuo yra fizinis asmuo – nuolat gyvenantis ar turintis pilietybę) šio įstatymo 92 straipsnio 14 dalyje numatytame sąraše nurodytose valstybėse ar teritorijose;

2) techninės ar programinės įrangos priežiūra ar palaikymas būtų vykdomas iš šio įstatymo 92 straipsnio 14 dalyje numatytame sąraše nurodytų valstybių ar teritorijų.“

Susijusi informacija

- Skenuoti originalai (1)
- Teisės akto pakeitimai (0)
- Pakeistas dokumentas (1)
- Susiję dokumentai (1)

<...> šilumos energijos tiekimas ne mažiau kaip 10000 vartotojų;

Santykis su asmens duomenų saugumo reikalavimais pagal ES Bendrąjį duomenų apsaugos reglamentą (BDAR)

Organizacinės asmens duomenų saugumo priemonės

AD saugumo politika ir procedūros
(saugumo politika ir jos peržiūra)

Vaidmenys ir atsakomybės
(aiškus apibrėžimas ir paskirstymas. Saugos spec. paskyrimas)

Prieigos valdymo politika
("būtina žinoti". Dokumentavimas)

Išteklių ir turto valdymas
(IT išteklių registras, išteklių peržiūra)

Pakeitimų valdymas
(pakeitimai stebimi, specialioje aplinkoje, pagal pakeitimų politiką)

Duomenų tvarkytojai
(duomenų tvarkytojų kontrolė, procedūrų apibrėžimas, tikrinimas)

AD saugumo pažeidimai ir kibernetiniai incidentai
(procedūros, pranešimas vadovybei, fiksavimas)

Veiklos tęstinumas
(veiklos tęstinumo planas)

Personalo konfidencialumas
(informavimas apie atsakomybes. Įpareigojimas laikytis konfidencialumo sąlygų)

Mokymai
(darbuotojų / naujų darbuotojų mokymai/ Mokymų planas)

Reikalavimai dėl tinkamų organizacinių duomenų saugumo priemonių

Eil. Nr.	Reikalavimas	Atitikmuo ISO 27001:2017 A priede	Atitikmuo BDAR ir paaiškinimai
	Asmens duomenų saugumo politika ir procedūros		
1.	Asmens duomenų ir jų tvarkymo saugumas organizacijoje turi būti dokumentuotas kaip informacijos saugumo politikos dalis.	**A.5 Informacijos saugumo politika**	Saugumo politika yra svarbus dokumentas, nustatantis pagrindinius informacijos saugumo ir asmens duomenų apsaugos principus organizacijoje. Tai yra visų konkrečių techninių ir organizacinių duomenų saugumo priemonių įgyvendinimo pagrindas pagal BDAR 32 straipsnį ir jį papildantį 24 straipsnį dėl duomenų valdytojo įgyvendinamos atitinkamos duomenų apsaugos politikos. Remiantis saugumo politika, konkrečios techninės ir organizacinės priemonės aprašomos detalesnėse politikose (pvz., prieigos kontrolės, įrenginių valdymo, išteklių valdymo ir kt.). Saugumo politika nustato bendrą organizacijos informacijos saugos valdymą ir gali būti dalis bendros organizacijos IT saugos politikos. Bet kuriuo atveju saugumo politikoje turi būti aiškiai išskirta asmens duomenų apsauga.
2.	Saugumo politika turi būti peržiūrima ir prireikus atnaujinama ne rečiau kaip kartą per metus.		
3.	Organizacija turi dokumentuoti atskirą, specialią saugumo politiką, susijusią su asmens duomenų tvarkymu. Šią politiką turi patvirtinti vadovybė ir perduoti visiems darbuotojams ir atitinkamiems išorės subjektams.		

Kiekvienam asmeniui - konkrečios prieigos teisės pagal **"būtina žinoti"** principą

Detali ir dokumentuota prieigos kontrolės politika. Prieigos funkcijų atskyrimas

Apibrėžtos pareigybės su didel. prieigos teisėmis. Priskirta tik ribotam darbuotojų skaičiui

Organizacinių saugumo priemonių kai kurie praktiniai niuansai

• Silpna duomenų tvarkytojų kontrolė / duomenų tvarkytojų kontrolės nebuvimas / aktualaus duomenų tvarkytojų sąrašo neturėjimas.
• Privilegijuotų vartotojų (pvz., sistemų administratorių) kontrolės nebuvimas.
• Už kibernetinį saugumą atsakingų asmenų nepaskyrimas.
• Saugumo / kibernetinio saugumo mokymų nevykdymas.
• Nenustatytos ir dokumentais nepatvirtintos slaptažodžių naudojimo taisyklės / neturėjimas vieningos slaptažodžių politikos.
• Atsarginių kopijų darymo ir veiklos tęstinumo politikos trūkumai.
• Trūkumai dėl IT teikėjų saugumo valdymo politikos.
• Nėra mobiliųjų įrenginių naudojimo politikos.
• Avarinio asmens duomenų atkūrimo tvarkos nebuvimas.
• Nešifruojami nešiojami kompiuteriai.
• Registracijos žurnalų serverinėje nebuvimas.
• Įrangos utilizavimo politikos nebuvimas ir kt.

Techninės asmens duomenų saugumo priemonės

Prieigų kontrolė ir autentifikavimas
(įgyvendinta prieigų kontrolė. Reikalavimai slaptažodžiams. Autentifikavimas)

Techninių žurnalų įrašai ir stebėsena
(darbuotojų ir adm. veiksmų fiksavimas. Stebėsena)

Tarnybinių stočių, duomenų bazių apsauga
(tinkama konfigūracija, pseudonimizav. ir kt.)

Darbo vietų apsauga
(antivirus. program. atnaujinimas, draudimas iškelti duomenis ir kt.)

Tinklo ir komunikacijos apsauga
(reikalavimai belaidžiam tinklui, IS tinklo atskyrimas ir kt.)

Atsarginės kopijos
(stebėjimas, reguliarumas, šifravimas ir kt.)

Mobilieji, nešiojami įrenginiai
(mobiliųjų įrenginių registravimas, autorizavimas, šifravimas ir kt.)

Programinės įrangos sauga
(reikalavimai saugumui, prasiskverbimo testavimai)

Duomenų naikinimas, šalinimas
(fizinis laikmenų naikinimas, išmagnetinimas)

Fizinė sauga
(darbuotojų ir kitų asmenų iidentifikavimas, gaisro gesinimo sistema ir kt.)

Reikalavimai dėl tinkamų techninių duomenų saugumo priemonių

	Reikalavimas	Atitikmuo ISO 27001:2017 A priede	Atitikmuo BDAR ir paaiškinimai, galimos grėsmės
	Prieigų kontrolė ir autentifikavimas		
42.	Turi būti įdiegta, įgyvendinta Prieigų kontrolės sistema, kuri taikoma visiems IT sistemos naudotojams. Prieigų kontrolės sistema turi leisti kurti, patvirtinti, peržiūrėti ir panaikinti naudotojų paskyras.	**A.9 Prieigos valdymas**	Prieigų kontrolė ir autentifikavimas yra esminiai saugos reikalavimai, siekiant apsisaugoti nuo neautorizuotos prieigos prie IT sistemos, kurioje yra tvarkomi asmens duomenys. Šie saugos reikalavimai įgyvendina organizacijos prieigų kontrolės politiką (taip pat žiūrėti šių gairių 12–15 punktus „Prieigos valdymo politika“) techniškai panaudojant specifinius, techninius komponentus ir taikomąsias programas. **Galimos grėsmės ir pavojai** Nesukontroliuojamos neautorizuotų naudotojų prieigos prie asmens duomenų; neautorizuotas duomenų bazės turinio (asmens duomenų) atskleidimas, **peržiūrėjimas, kopijavimas, redagavimas, naikinimas (angl.** *broken access control; broken authentification*). Naudotojų atliktų veiksmų kontrolė, atsekamumas bendroje paskyroje; naudotojo prisijungimo duomenų prie bendros paskyros atskleidimas; neteisėtas bendros paskyros naudotojo teisių eskalavimas į aukštesnes pareigas (administratoriaus). Neteisėto turinio kaupimas ir vykdymas. Sudėtingas naudotojų atliktų veiksmų atsekamumas nesant autentifikacijos, autorizacijos mechanizmo; neautorizuotos naudotojų prieigos prie duomenų bazės turinio (asmens duomenų); neautorizuotas asmens duomenų peržiūrėjimas, kopijavimas, redagavimas, naikinimas. IT infrastruktūros, informacinių sistemų, duomenų bazės tiesioginė prieiga kompiuterių tinklais, internetu, be autorizacijos. Neužtikrinama, nesukontroliuojama slaptažodžių politika; nesilaikoma
43.	Turi būti vengiama naudoti bendras naudotojų paskyras. Vietose, kur bendra naudotojų paskyra yra būtina, turi būti užtikrinta, kad visi bendros paskyros naudotojai turi tokias pat teises ir pareigas.		
44.	Turi būti veikiantis autentifikavimo mechanizmas, leidžiantis prieigą prie IT sistemos (paremtas Prieigų kontrolės **politika). Minimalus reikalavimas** naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir slaptažodis. Slaptažodis sudaromas atsižvelgiant į tam tikrą kompleksiškumo lygį.		
45.	Prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti		

Techninių saugumo priemonių kai kurie praktiniai niuansai

- Nenaikinami asmens duomenys. Asmens duomenų iš KDV, el. pašto netrynimas, nearchyvavimas.
- Prieigų kontrolės trūkumai:
  - nuo iki beveik visiškos prieigų kontrolės nebuvimo.
  - administratorių prieigos nefiksuojamos.
  - darbuotojai, keičiantys pareigas, gali turėti senas prieigas prie sistemų.
  - neatliekama vartotojų inventorizacija.
  - **Prieigos teisių periodinė peržiūra** // **Prieigos teisių nenaikinimas**.
  - nebuvimas galimybių suteikti teises pagal roles.
- Prieigos principas „būtina žinoti“ (t.y. reikalinga funkcijoms vykdyti). Būtina dokumentuoti.
- Blogai formuojami slaptažodžiai, nekeičiami periodiškai arba keičiami per retai.
- Aukšto lygio sistemos nėra šifruojamos.
- Neatliekami periodiškai infrastruktūros atsparumo įsiskverbimui testavimai.
- Mobilieji įrenginiai neturi centralizuoto valdymo.
- Kiti aspektai: ar užtenka periodinių prasiskverbimo testų, kad aptikti „neapsaugotus“ asmens duomenis?

KIBERNETINIO SAUGUMO politikos ir jos įgyvendinimo DOKUMENTAI

• **ORGANIZACINIŲ IR TECHNINIŲ KIBERNETINIO SAUGUMO REIKALAVIMŲ, TAIKOMŲ KIBERNETINIO SAUGUMO SUBJEKTAMS, APRAŠAS (LRV nutarimas Nr. 818).**

• Subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojai <…> suderinę su Nacionaliniu kibernetinio saugumo centru, **tvirtina kibernetinio saugumo politikos ir jos įgyvendinimo dokumentus**, kuriuose turi būti nustatyta: <…> (*pastaba*: 5.3 p. – 28 papunkt.).

• Aprašo 5.3 papunkčio nuostatose nurodytą informaciją ar dokumentus turi teisę išdėstyti pagal Bendruosius elektroninės informacijos saugos reikalavimus rengiamuose ir tvirtinamuose saugos dokumentuose. Šiuo atveju paminėti saugos dokumentai derinami Bendruosiuose elektroninės informacijos saugos reikalavimuose nustatyta tvarka.

• Kibernetinio saugumo politikos ir jos įgyvendinimo dokumentai turi būti peržiūrimi (persvarstomi) ne rečiau kaip kartą per metus.

• Taip pat: valstybės informacinių išteklių veiklos tęstinumo valdymo planai ar kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planai.

5.3.1. kibernetinio saugumo politikos ir jos įgyvendinimo dokumentų taikymas ir naudojimas;

5.3.2. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų grupių sudarymas, teisių ir prieigos prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros paslaugų ir išteklių suteikimas ir valdymas;

5.3.3. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų pareigos ir funkcijos, susijusios su kibernetiniu saugumu;

5.3.4. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų, kompetentingo asmens ar padalinio, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, mokymai kibernetinio saugumo klausimais;

5.3.5. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų vardų ir slaptažodžių sudarymas, apsauga ir keitimas;

5.3.6. audito įrašų administravimas ir saugojimas;

5.3.7. įsibrovimų aptikimas ir prevencija;

5.3.8. saugus naudojimasis belaidžiu tinklu;

5.3.9. mobiliųjų įrenginių, naudojamų prisijungti prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, saugus naudojimas ir kontrolė;

5.3.10. duomenų, esančių mobiliuosiuose įrenginiuose, šifravimo nuostatos;

5.3.11. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros išteklių naudojimas už organizacijos ribų ir (arba) mobiliaisiais įrenginiais;

5.3.12. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudojamų svetainių saugos valdymas;

5.3.13. grėsmių ir pažeidžiamumų, galinčių turėti įtakos valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros kibernetiniam saugumui, vertinimas;

5.3.14. pažeidžiamumų nustatymo dalyvių teisės ir pareigos;

5.3.15. pažeidžiamumų nustatymo plano rengimas;

5.3.16. pažeidžiamumų nustatymo programinės įrangos naudojimas;

5.3.17. pažeidžiamumų nustatymo rezultatų klasifikavimas;

5.3.18. pažeidžiamumų nustatymo ataskaitų rengimas ir nustatytų trūkumų šalinimas;

5.3.19. kibernetinio incidento valdymo organizavimas;

5.3.20. kibernetinio incidento nustatymas;

5.3.21. kibernetinio incidento vertinimas;

5.3.22. kibernetinio incidento stabdymas ir šalinimas;

5.3.23. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros įprastinės veiklos atkūrimas ir maksimalus leistinas paslaugos neveikimo laikas;

5.3.24. įgytos kibernetinių incidentų valdymo patirties vertinimas;

5.3.25. kibernetiniam saugumui užtikrinti naudojamų priemonių diegimo ir šių priemonių parametrų keitimas;

5.3.26. Reikalavimų įgyvendinimo kontrolės ir atitikties vertinimas;

5.3.27. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros kibernetinio saugumo būklės gerinimas;

5.3.28. elektroninio pašto naudojimas.

Pagrindiniai pakeitimai LRV nutarime Nr. 716

• *LRV nutarimas 2018-01-03: Dėl Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimo Nr. 716 „**Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo**, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ pakeitimo.*

• Elektroninės informacijos sauga informacinėse sistemose turi atitikti KAM tvirtinamus Techninius informacinių sistemų elektroninės informacijos saugos reikalavimus.

• Informacinės sistemos valdytojas privalo turėti pagal Lietuvos Respublikos Vyriausybės patvirtintą Saugos dokumentų turinio gairių aprašą parengtus, su krašto apsaugos ministro įgaliota institucija, įgyvendinančia valstybės informacinių išteklių saugos politiką, suderintus ir patvirtintus šiuos saugos dokumentus <...>.

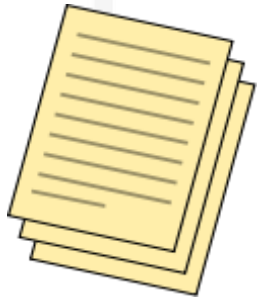
• Informacinės sistemos priskyrimas atitinkamai kategorijai derinimas su KAM įgaliota institucija.

Informacijos saugos politikos formavimas ir įgyvendinimas

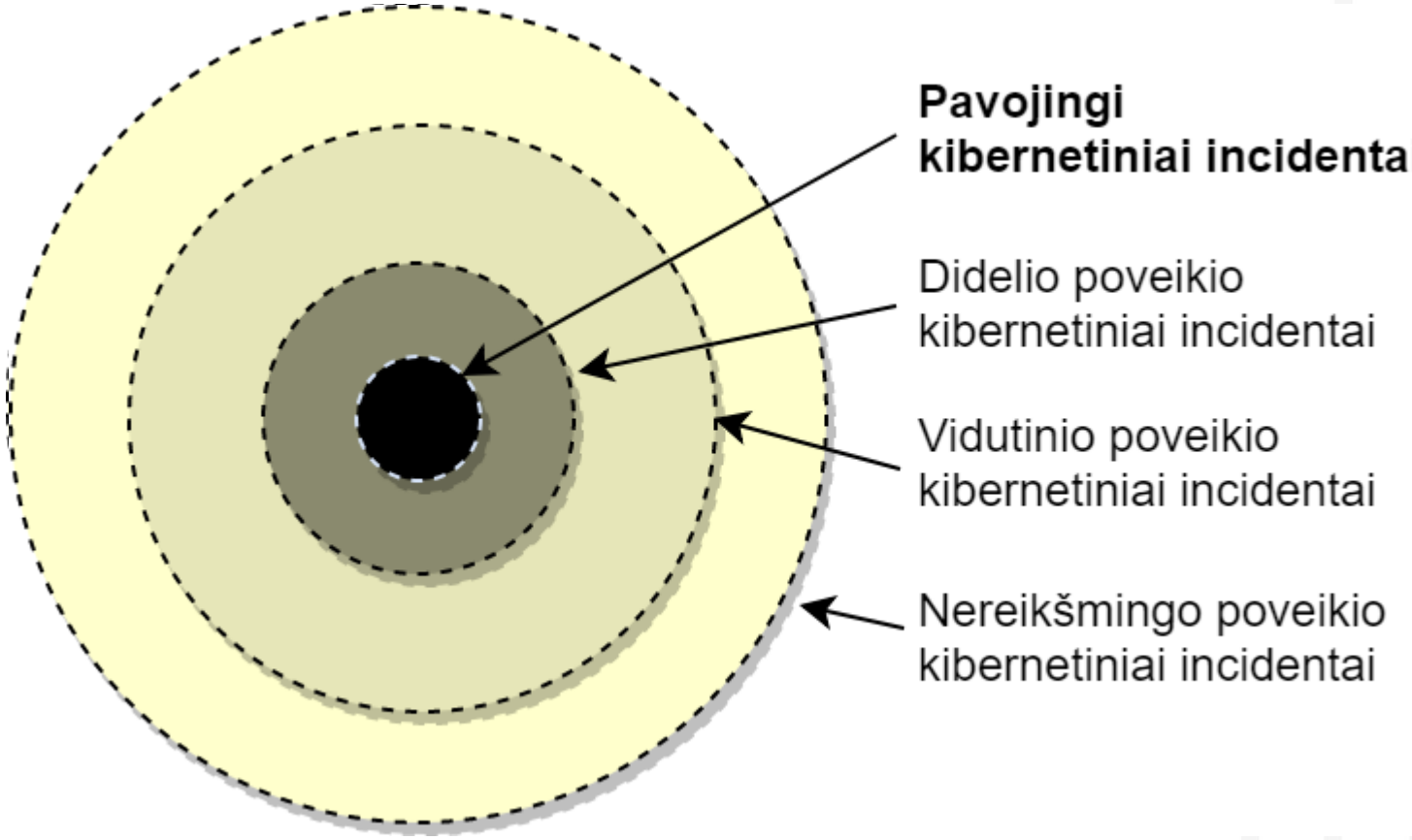
Privalomi saugos dokumentai ir jų turinys:

1. Informacinės sistemos duomenų saugos nuostatai.
2. Saugaus el. informacijos tvarkymo taisyklės.
3. Informacinės sistemos veiklos tęstinumo valdymo planas.
4. Informacinės sistemos naudotojų administravimo taisyklės.

Saugos dokumentų peržiūrėjimas: <...> turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per metus informacinės sistemos valdytojo vadovo nustatyta tvarka. Saugos dokumentai taip pat turi būti persvarstomi (peržiūrimi) po to, kai atliekamas rizikos įvertinimas ar informacinių technologijų saugos atitikties vertinimas arba institucijoje įvyksta esminių organizacinių, sisteminių ar kitokių pokyčių.



KIBERNETINIŲ INCIDENTŲ KLASIFIKACIJA (pagal Nacionalinį KI valdymo planą (2018 LRV nutarimo „Dėl KSĮ įgyvendinimo..“ dalis))



Pavojingas: pvz., sutrikimas daugiau nei 24 val. ir (ar) viršijamas max leidžiamas pasl. neveikimo laikas.
D poeikio: pvz., aptinkama moderni kenkimo įranga (kompiuterizuotų vietų skaičius daugiau nei 25%).
V poveikio: pvz., aptinkamas paslaugos trikdymas, kuris neturi įtakos paslaugų teikimui, daugiau nei 1 val.
N poveikio: pvz, nepageidaujamų laiškų, klaidinančios informacijos platinimas.

- Kibernetinius incidentus Plano 9.2–9.4 papunkčiuose nustatytoms kategorijoms, atsižvelgdami į Plano priede nustatytus kriterijus, **priskiria kibernetinio saugumo subjektai**.
- Kibernetinius incidentus Plano 9.1 papunktyje nustatytai **pavojingo** kibernetinio incidento kategorijai turi teisę priskirti **tik Nacionalinis kibernetinio saugumo centras**, jeigu nustatytas kibernetinis incidentas ir (ar) jo poveikis atitinka bent vieną iš kriterijų, nurodytų Plano priede, būdingų pavojingo incidento kategorijai.

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)			
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 %	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 %	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 %	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos neveikimo laikas	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 100 000, arba 50 % [illegible]	visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje, valstybės funkcijų ir (ar) prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus įvykis, nurodytas Vyriausybės patvirtintame Ekstremaliųjų įvykių kriterijų
	prisijungti prie RIS, ją užvaldyti ir kontroliuoti, sutrikdyti ar pakeisti jų veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę ja naudotis ir neteisėtai pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją tokios teisės neturintiems asmenims	durys“ (angl. *back door*), kompiuterizuotos darbo vietos ar tarnybinės stotys tampa „Botinklo“ (angl. *Botnet*) infrastruktūros dalimi																		
		2.3. Kenkimo programinė įranga, trikdanti saugumo priemonių darbą					V					D					P			
		2.4. Kenkimo programinė įranga, kurią aptinka saugumo priemonės per reguliarų patikrinimą ir (ar) kurią saugumo priemonės automatiškai blokuoja	N				V													
		2.5. Kenkimo programinė įranga, platinama naudojant socialinės inžinerijos metodus	N				V					D					P			
3.	Informacijos rinkimas (angl. *information gathering*)	3.1. RIS paketų / informacijos perėmimas					V					D					P			

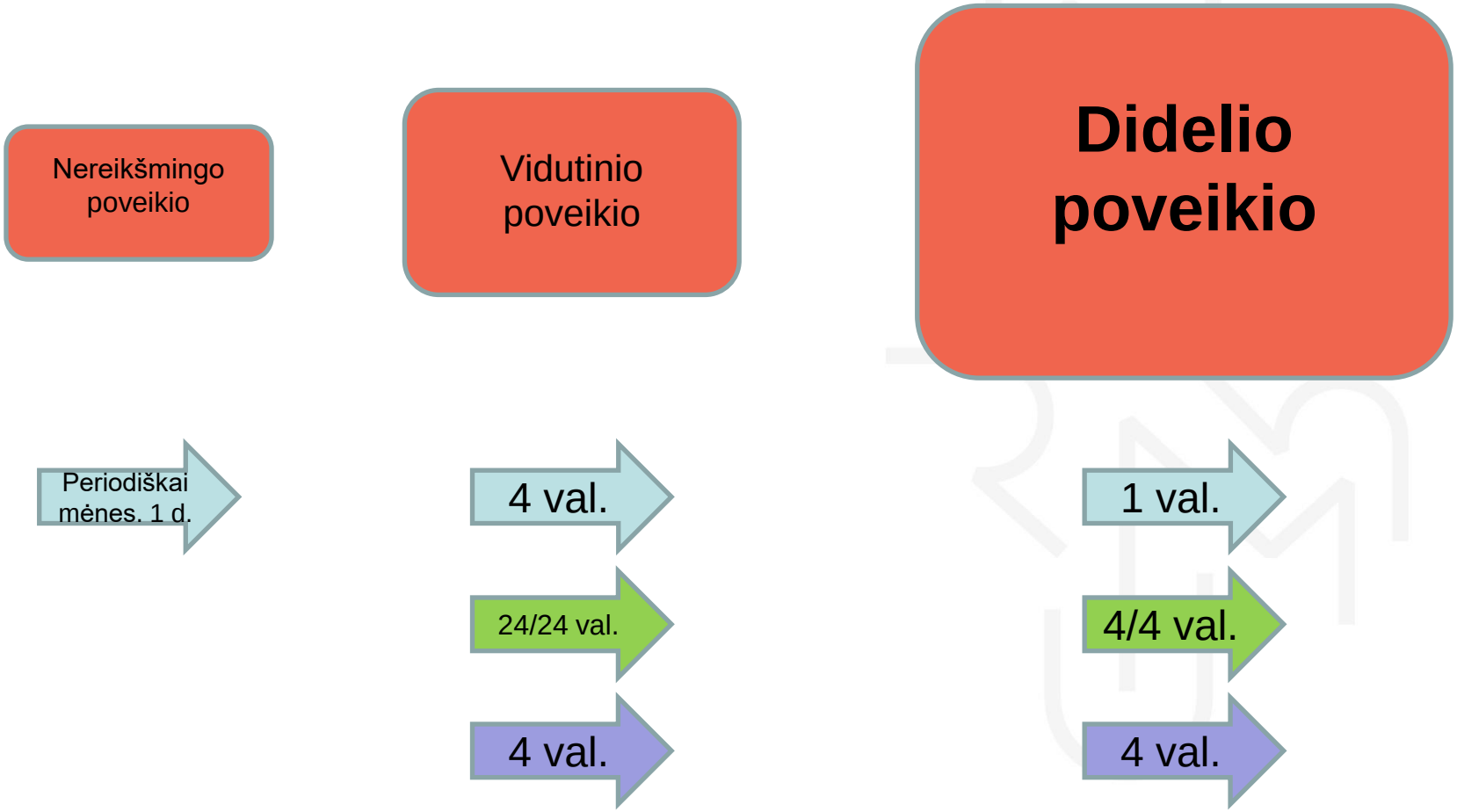
PRANEŠIMAS APIE KIBERNETINIUS INCIDENTUS

- **Kibernetinis incidentas –** *įvykis ar veika, kuri sukelia ar gali sukelti neteisėtą prisijungimą ar sudaryti sąlygas neteisėtai prisijungti prie informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos, sutrikdyti ar pakeisti, įskaitant valdymo perėmimą, informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, taip pat sudaryti sąlygas pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją tokios teisės neturintiems asmenims*.
- *Pareigos apie kibernetinius incidentus informuoti*:
  - NKSC;
  - ~~RRT~~;
  - ~~VDAI~~ (kiek tai susiję su AD);
  - Policijai (kiek tai susiję su tyrimu).

Pranešimas apie kibernetinį incidentą NKSC

- Pareiga pranešti – kibernetinio saugumo subjektams (*anksčiau buvo: viešojo administravimo subjektams bei YSII*).
- Apie kibernetinius incidentus, pagal Nacionalinį kibernetinių incidentų valdymo planą (*patvirtinta 2018-12-05 LRV nutarimu Nr. 1209*).
- Atsakomybė: už informacijos nepateikimą arba teikimo tvarkos pažeidimą – įspėjimas arba bauda JA vadovams ar kitiems asmenims iki 300 EUR (pagal ANK 479 str.).
- Pakartotinai – iki 1440 EUR.
- Problema – KS`tai dažniausiai mano, kad kibernetiniai incidentai nereikšmintg!

Kibernetinių incidentų kategorijos // pranešimas NKSC, ataskaitos pateikimas/atnaujinimas, suvaldymas/pasibaigimas (*pagal Nacionalinį kibernetinių incidentų valdymo planą (buv. pagal organizacinius ir techninius reikalavimus*))



Reikalavimai pranešimo turiniui

14. Nacionalinis kibernetinio saugumo centras informuojamas **apie didelio ar vidutinio poveikio** kibernetinius incidentus kibernetinio saugumo subjekto pranešimu, kuriame **nurodoma**:

14.1. kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija, nustatyta pagal Plano priede pateiktus kriterijus;

14.2. trumpas kibernetinio incidento apibūdinimas;

14.3. tikslus laikas, kada kibernetinis incidentas įvyko ir buvo nustatytas;

14.4. kibernetinio incidento šalinimo tvarka (nurodant, ar tai prioritetas, ar ne);

14.5. tikslus laikas, kada bus teikiama kibernetinio incidento tyrimo ataskaita.

NKSC, gavęs pranešimą, gali prašyti patikslinti arba papildomos informacijos.

Reikalavimai ataskaitai apie kibernetinį incidentą

24. Nacionaliniam kibernetinio saugumo centrui teikiant **didelio ar vidutinio poveikio** kibernetinio incidento tyrimo **ataskaitą nurodoma** kibernetinio saugumo subjektui žinoma informacija:

24.1. kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija, nustatyta pagal Plano priede pateiktus kriterijus;

24.2. ryšių ir informacinės sistemos, kurioje nustatytas kibernetinis incidentas, tipas (elektroninių ryšių tinklas, informacinė sistema, registras, pramoninių procesų valdymo sistema, tarnybinė stotis ir panašiai);

24.3. kibernetinio incidento veikimo trukmė;

24.4. kibernetinio incidento šaltinis;

24.5. kibernetinio incidento požymiai;

24.6. kibernetinio incidento veikimo metodas;

24.7. galimos ir (ar) nustatytos kibernetinio incidento pasekmės;

24.8. kibernetinio incidento poveikio pasireiškimo (galimo išplitimo) mastas;

24.9. kibernetinio incidento būsena (aktyvus, pasyvus);

24.10. priemonės, kuriomis kibernetinis incidentas nustatytas;

24.11. galimos ir (ar) taikomos kibernetinio incidento valdymo priemonės;

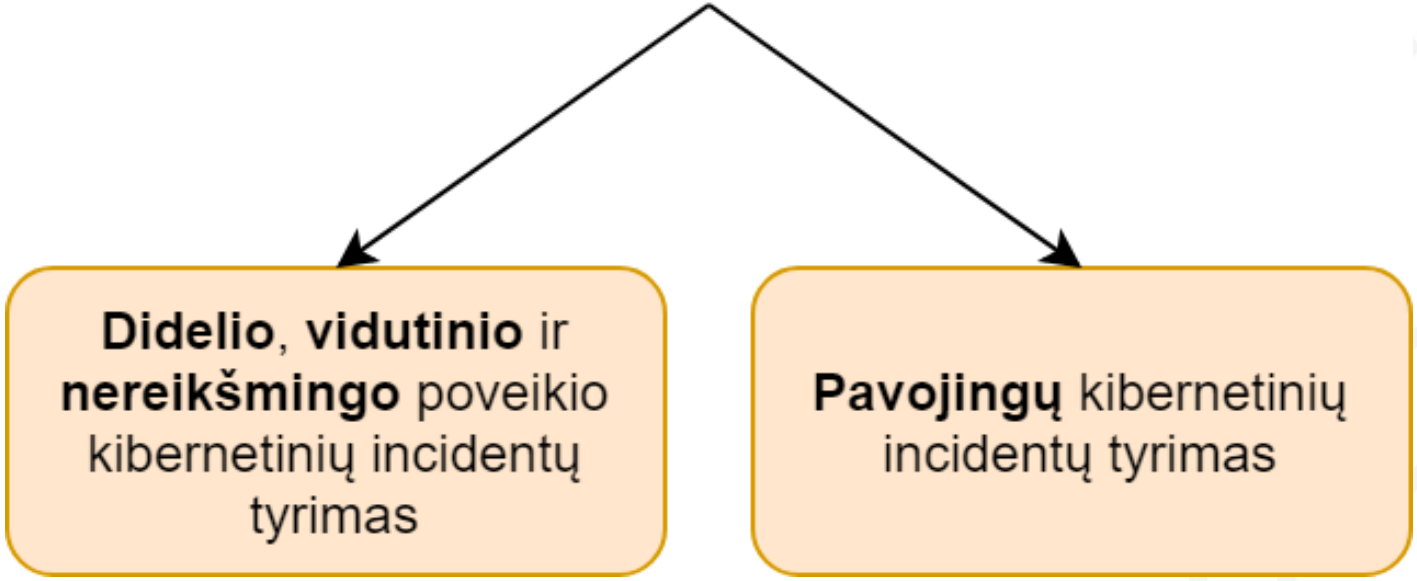
24.12. tikslus laikas, kada bus teikiama pakartotinė kibernetinio incidento tyrimo ataskaita remiantis Plano 23 punktu.

Išimtys dėl pranešimo apie incidentus bei kitos pareigos

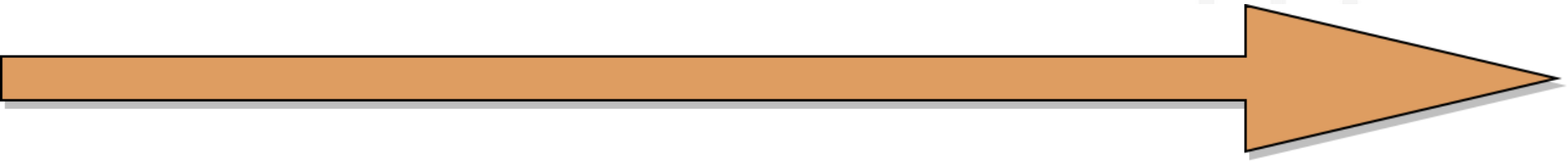
- **Skaitmeninių paslaugų teikėjai** – tik apie didelio poveikio kibernetinius incidentus ir tik tuo atveju, kai gali pasinaudoti informacija, reikalinga incidento poveikiui įvertinti.
- **YSII** (*kai paslaugų teikimas priklauso nuo skaitmeninių paslaugų teikėjų paslaugų*), nustatę neigiamą poveikį YSII, ne vėliau kaip per vieną valandą informuoja NKSC bei atitinkamus SPT.
- **Kiti asmenys** – turi teisę pranešti NKSC savanoriškai (tokiu atveju kategorijas priskiria NKSC).
- **NKSC** ne vėliau kaip per 1 val. informuoja pareiškėją apie patikslintą/priskirtą kibernetinio incidento kategoriją.
- (*kai būtina informuoti visuomenę, siekiant išvengti ar valdyti KI*) **NKSC** (pasitaręs su kibernetinio saugumo subjektu) informuoja visuomenę apie pavienius kibernetinius incidentus arba reikalauja kad tai padarytų **kibernetinio saugumo subjektas**.

KIBERNETINIŲ INCIDENTŲ TYRIMAS

• Tipinis kibernetinių incidentų valdymo YSII planas (LRV 2016-07-20 Nr. 746) – neteko galios nuo 2018-12-31.
• Nacionalinis kibernetinių incidentų valdymo planas (Planas) koreguotas 2018 m.
• Pagal Planą, kibernetinių incidentų tyrimas:



Didelio, vidutinio, nereikšmingo pobūdžio kibernetinių incidentų tyrimas



Kibernetinio saugumo subjektai atlieka kibernetinio incidento tyrimą, kaip tai reglamentuota KS dokumentais. Imasi būtinų priemonių suvaldyti ir veiklai atkurti

Kibernetinio saugumo subjektai NKSC pateikia incidento tyrimo ataskaitą (*terminai*)

Kibernetinio saugumo subjektai, įvertinę, kad negalės ištirti ar suvaldyti per vid. dokumentuose nustatytus terinus, per 24 val. kreipiasi pagalbos į NKSC

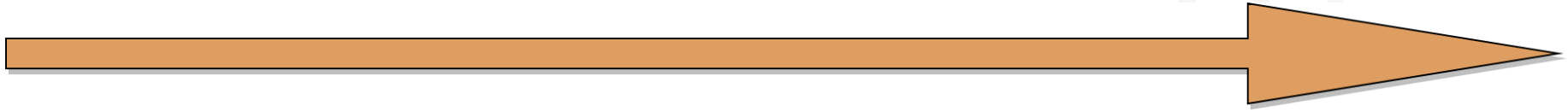
NKSC imasi būtinų priemonių ištirti ir aplinkybėms išsiaiškinti

Didelio ir vidutinio poveikio atveju, incidentas laikomas suvaldytu ar pasibaigė kai išnyksta vid. dokumentuose nustatytas poveikis

Kibernetinio saugumo subjektai per 8 val. nuo suvaldymo ar pasibaigimo informuoja paslaugų gavėjus, jei kilo žala ar ateity gali kilti

Pareiga kibernetinio saugumo subjektams NKSC pateikti atsakingų asmenų kontaktinius duomenis (turi būti pasiekiami visą parą). Pasikeitus informuoti per 1 d.d.

Pavojingų kibernetinių incidentų tyrimas



NKSC, priskyręs pavojingo incidento kategorijai, per 1 val. **informuoja** KIVT institucijas ir **nurodo** subjektams, kad incidentas tiriamas pagal subjektų teisės aktus arba perima inc. tyrimą ir (ar) valdymo organizavimą

Kibernetinio saugumo subjektai ne rečiau kaip kas 4 val. NKSC **teikia** informaciją apie incidento būklę (*nurodo informaciją kaip ir teikiant inc. ataskaitą*). NKSC gali perimti incidento tyrimą ir (ar) valdymo organizavimą

NKSC perėmus tirti ir (ar) organizuoti inc. valdymą, kibernetinio saugumo subjektai: renka, apdoroja informaciją ir ne rečiau kaip kas 4 val. teikia NKSC informaciją apie incidentą bei tyrimo/valdymo veiksmus (*forma kaip ir ataskaita*). Taip pat vykdo NKSC nurodymus, dalyvauja inc. valdyme.

NKSC perėmęs inc. tyrimą ir (ar) valdymo organizavimą: vertina, priima sprendimus, duoda nurodymus. NKSC turi teisę surengti koordinacinį pasitarimą (kibernetinio saugumo subjektai, KIVT, kiti subjektai, ekspertai). Pirmiausia valdomi incidentai, keliantys didžiausią žalą

NKSC apie eigą nedelsiant, bet ne vėliau kaip per vieną valandą **informuoja**: LRV, Seimo ir Prezidento kanceliarijų, KAM paskirtus atsakingus asmenis ir per 4 val. **pateikia** apibendrintą ataskaitą

LRV, Seimo, Prezidento kanceliarijos informuoja atitinkamai vadovus, Ministrą pirmininką, Seimo pirmininką, Prezidentą.

NKSC reguliariai ne rečiau kaip kas 4 val. informuoja nurodytus gavėjus. Apie pasibaigimą ar suvaldymą informuoja apie pasibaigimą/ suvaldymą (kai išnyksta poveikis ir (ar) atkuriama įprasta veikla

Jei nepakanka resursų, per 1 val. **NKSC informuoja** LRV kanceliarijos, KAM paskirtus atsakingus asmenis, KA ministrą. **KA ministras** per 24 val. **priima sprendimą** dėl priemonių. Nesuvaldžius, per 1 val. **informuojamas ministras ir LRV kanceliarija** (*ir pateikiama ataskaita*)

KA ministras per 24 val. nuo informacijos gavimo **teikia** LRV nutarimo projektą dėl pripažinimo kibernetinio saugumo krize (*PS: krizės valdymui vadovauja LRV)*

Kibernetinių incidentų analizė baigus tyrimą

- **Pareiga** kibernetinio saugumo subjektams ir KIVT po kibernetinio incidento suvaldymo ar pasibaigimo **atlikti** jo **analizę** (išskyrus nereikšmingo poveikio).
- Procedūra kibernetinio saugumo subjektams:
  - Per 30 d.d. pateikia NKSC analizės rezultatus ir informaciniame tinkle paskelbia susistemintą, aktualią ir neįslaptintą informaciją apie nustatymą ir suvaldymą;
  - Imasi priemonių, kad būtų pašalintas pažeidžiamumas;
  - Įvertina RIS riziką ir atitiktį org.-tech. reikalavimams;
  - Nustačius teisinio reglamentavimo spragų, keičia teisės aktus ar inicijuoja teisės aktų pakeitimus.
- KIVT per 30 d.d. nuo suvaldymo/pasibaigimo **gali pareikalauti** kibernetinio saugumo subjekto papildomos informacijos.
- **KIVT institucijos**: keičia (inicijuoja) teisės aktus/pakeitimus; (prireikus) inicijuoja YSII kibernetinės gynybos plano pakeitimus; įvertina org.-tech. tobulinimo poreikį.

RIZIKOS VERTINIMAS ARSIS METODU

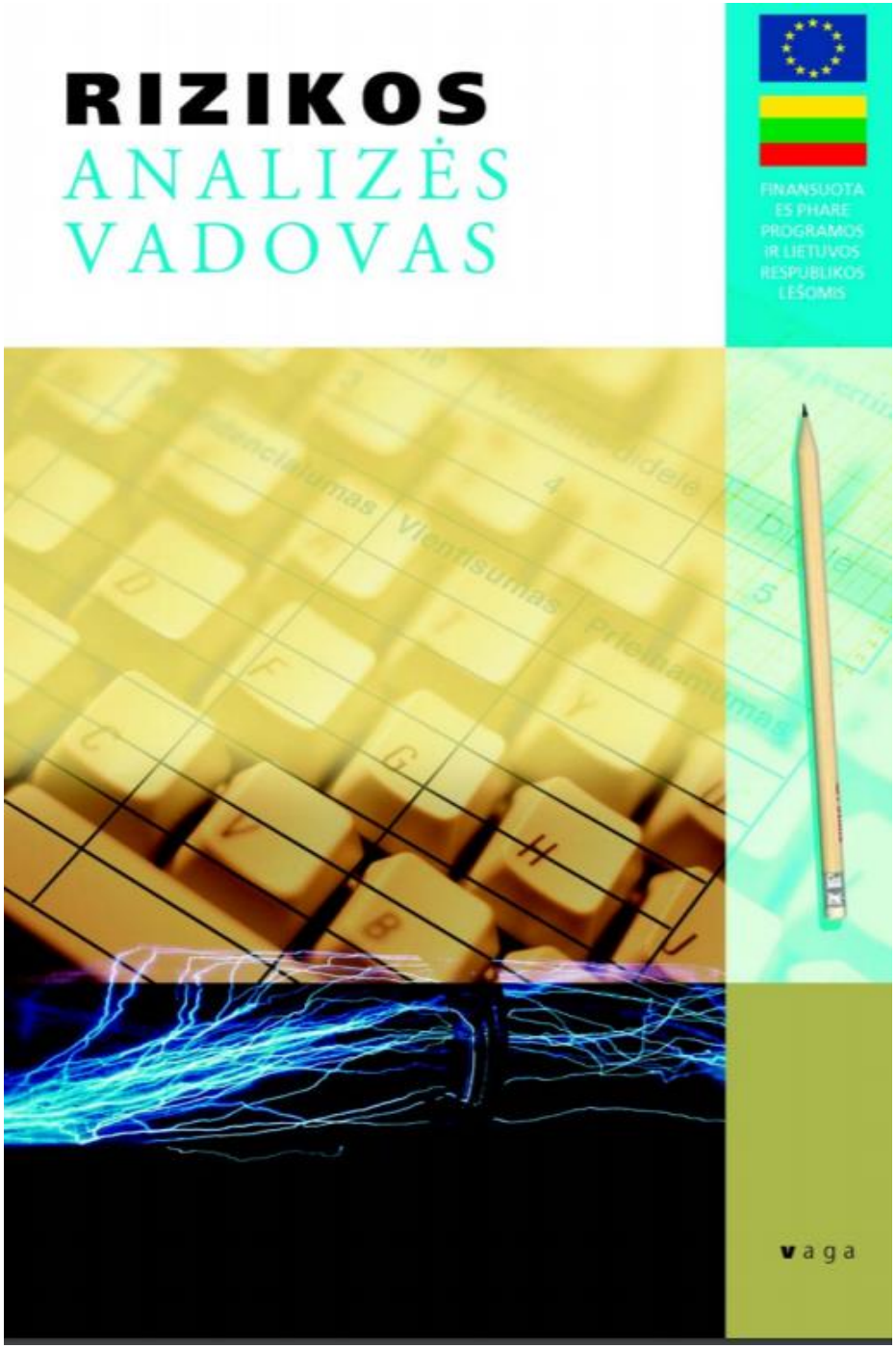
Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos (ARSIS) paslaugos

Prisijungti prie ARSIS >>>

Prašymų užregistruoti ARSIS naudotoją ir suteikti jam prieigą prie ARSIS pateikimas.

Prašymo ir pasižadėjimo originalus, pasirašytus įprastu arba elektroniniu parašu valstybės informacinių išteklių (valstybės ar žinybinio registro, valstybės ar kitos informacinės sistemos) valdytojas turi raštu pateikti Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos. Rašte prašome nurodyti, kurių valstybės informacinių išteklių duomenis tvarkyti ir teikti yra suteikiamas įgaliojimas ARSIS naudotojui.

Prašymo įregistruoti ARSIS naudotoju šablonas
Pasižadėjimo laikytis ARSIS asmens duomenų apsaugos reikalavimų šablonas



https://vrm.lrv.lt/uploads/vrm/documents/files/LT_versija/Veikla/Veiklos%20sritis/Elektronin%C4%97_vald%C5%BEia/Elektronin%C4%97s_informacijos_sauga/Rizikos_analizes_vadovas.pdf

Kiekvieno darbuotojo indėlio užtikrinant asmens duomenų saugumą reikšmė