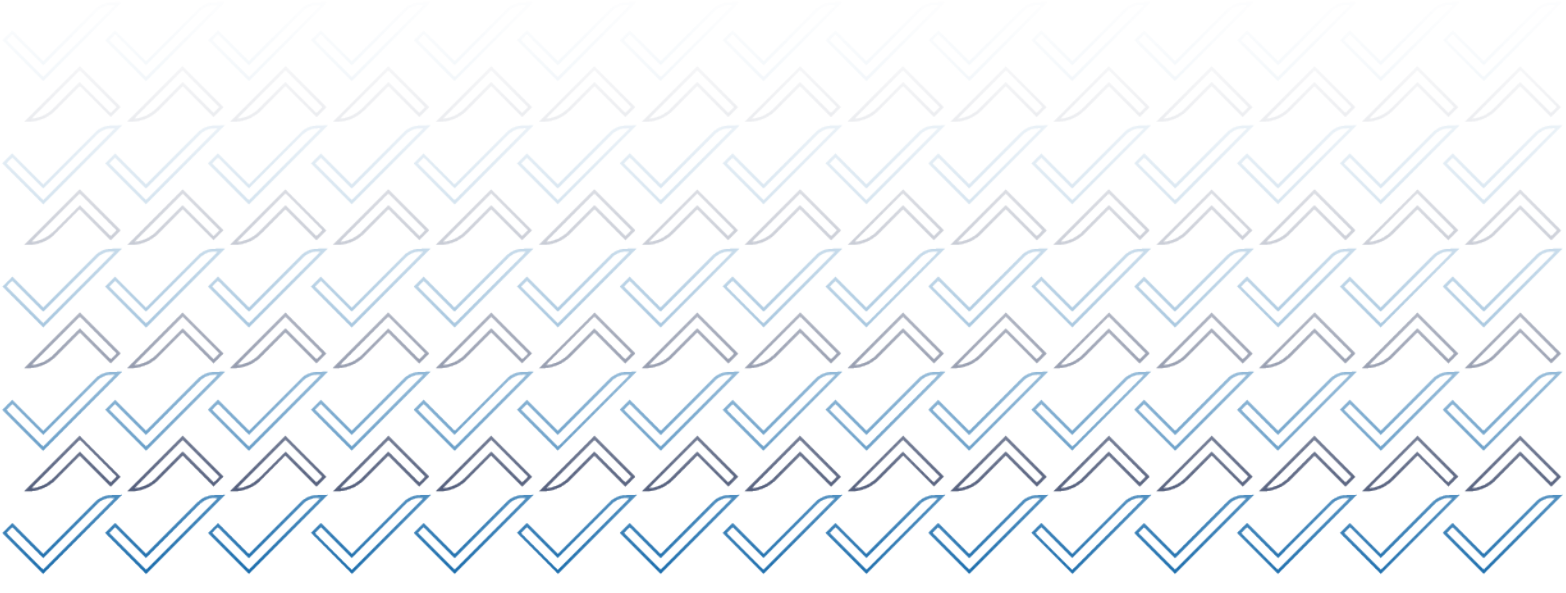
VALSTYBĖS KONTROLĖ
VALSTYBINIS AUDITAS

VALSTYBINIO AUDITO ATASKAITA

KIBERNETINIO SAUGUMO UŽTIKRINIMAS

2022 m. spalio 27 d.

Nr. VAE-10



Valstybės kontrolė – aukščiausioji valstybinio audito institucija – prižiūri, ar teisėtai ir efektyviai valdomas ir naudojamas valstybės turtas ir kaip vykdomas valstybės biudžetas. Valstybės kontrolė, teikdama audito pastebėjimus ir rekomendacijas, skatina teigiamą ir veiksmingą valstybinio audito poveikį valstybės finansų valdymo ir kontrolės sistemai bei į rezultatus ir visuomenės poreikius orientuotam viešajam valdymui. Daugiau apie Valstybės kontrolės veiklą ir valstybinio audito rezultatus – interneto svetainėje www.valstybeskontrole.lt.

Audito grupė: Markas Marcinkevičius (departamento vadovas), Diana Nikitina (grupės vadovė nuo 2022-05-27), Gytis Tamulevičius, Kristina Kielaitė-Talaikė, Evelina Petkevičiūtė, Jaroslav Rimoit, Vitoldas Vitkovskis.

Valstybinio audito ataskaita pateikta: Lietuvos Respublikos Seimo Audito komitetui, Nacionalinio saugumo ir gynybos komitetui, Krašto apsaugos ministerijai, Nacionaliniam kibernetinio saugumo centrui.

TURINYS

PAGRINDINIAI FAKTAI

6 vietoje

Lietuva tarp pasaulio valstybių pagal 2021 m. Jungtinių Tautų Tarptautinės telekomunikacijų sąjungos paskelbtą kibernetinio saugumo indeksą.

11 659

kibernetiniai incidentai registruoti Nacionalinio kibernetinio saugumo centro 2019–2021 m.

9 705,1 tūkst. Eur

asignavimų planuota kibernetinio saugumo stiprinimo priemonėms 2019–2021 m.

38 proc.

iš 212 apklaustų valstybės informacinių išteklių valdytojų ir tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų neatliko kibernetinio saugumo rizikų vertinimo 2019–2021 m.

81 proc.

(iš 403 valstybės informacinių išteklių) informacinių technologijų saugos atitikties vertinimo ataskaitų nepateikta Nacionaliniam kibernetinio saugumo centrui 2021 m.

7 metus

nuo 2016 m. rengiamas vieningos elektroninės informacijos saugos ir kibernetinio saugumo reikalavimų sistemos projektas.

35 proc.

iš 212 apklaustų valstybės informacinių išteklių valdytojų ir tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų nė karto nedalyvavo nacionalinėse kibernetinio saugumo pratybose 2019–2021 m.

11

iš 28 Nacionalinės kibernetinio saugumo strategijos tarpinstituciniame veiklos plane numatytų kibernetinio saugumo stiprinimo priemonių neįgyvendinta 2019–2021 m.

SANTRAUKA

Audito svarba

Ypatingos svarbos informacinė infrastruktūra, valstybės informacinių išteklių elektroninė informacija ir jų pagrindu veikiančios sistemos ir paslaugos yra gyvybiškai svarbios Lietuvos Respublikai. Dėl didėjančio paslaugų ir procesų skaitmenizavimo, COVID-19 pandemijos, geopolitinių iššūkių ir įtampų auga kibernetinių ir hibridinių atakų grėsmė, didėja jų socialinis ir ekonominis poveikis. Nacionalinio kibernetinio saugumo centro duomenimis [1], per 3 pastaruosius metus užregistruota 11 659 kibernetinių incidentų: 2019 m. – 3 241, 2020 m. – 4 330, 2021 m. – 4 088. Dėl didelio kibernetinių incidentų skaičiaus, jų modernėjimo, galimos rizikos patirti reikšmingus kibernetinių atakų ir incidentų padarinius, vis svarbiau užtikrinti kibernetinį saugumą nacionaliniu lygmeniu.

Kibernetinio saugumo užtikrinimas grindžiamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos ypatingos svarbos informacinės infrastruktūros, ryšių ir informacinių sistemų saugumui, rizikos vertinimu. Rizikos valdymas sudaro pagrindą veiksmingos saugumo reikalavimų valdymo sistemos sukūrimui, diegimui, palaikymui ir tobulinimui. Saugumo valdymo sistema apima institucijų, organizacijų tinklų ir informacinių sistemų saugumo reikalavimų (priemonių, taisyklių ir procedūrų) nustatymą ir vykdymą, stebėseną ir peržiūrą (atitikties vertinimą), kibernetinių incidentų prevenciją, aptikimą, reagavimą į juos, atsigavimą, atsako į kibernetinius incidentus galimybių, jų išvengimo priemonių vertinimą, saugumo technologijų valdymą, darbuotojų mokymą, informuotumo programas.

Suprasdami, kad kibernetinio saugumo rizikos valdymas, kibernetinių incidentų valdymas, prevencinė veikla, įskaitant kibernetinio saugumo pratybas ir mokymus, yra svarbūs veiksmingos saugumo valdymo sistemos elementai (veiksniai), lemiantys kibernetinio saugumo užtikrinimą, nusprendėme atlikti valstybinį auditą.

Audito tikslas ir apimtis

Audito tikslas – įvertinti, ar užtikrinamas kibernetinis saugumas.

Pagrindiniai audito klausimai:

- ar užtikrinamas kibernetinio saugumo rizikos valdymas nacionaliniu lygiu;
- ar kibernetinio saugumo teisinis reguliavimas ir atitikties teisės aktų nustatytiems reikalavimams vertinimo sistema veiksminga;
- ar užtikrinamas kibernetinių incidentų valdymas;
- ar užtikrinamas nuoseklus kibernetinio saugumo planavimo įgyvendinimas.

Audituojamieji subjektai:

[1] Prieiga per internetą: https://www.nksc.lt/aktualu.html (Nacionalinio kibernetinio saugumo būklės ataskaitos, žiūrėta 2022-07-08).

- Krašto apsaugos ministerija, nes formuoja kibernetinio saugumo politiką, organizuoja, kontroliuoja ir koordinuoja jos įgyvendinimą[2];
- Nacionalinis kibernetinio saugumo centras, nes įgyvendina kibernetinio saugumo politiką ir yra atsakingas už kibernetinių incidentų stebėseną ir rizikos kibernetinėje erdvėje analizę nacionaliniu lygmeniu, kibernetinio saugumo reikalavimų įgyvendinimo stebėseną, kibernetinio saugumo subjektų saugumo būklės įvertinimą[3].

Audito metu informaciją rinkome iš Krašto apsaugos ministerijos, Nacionalinio kibernetinio saugumo centro, atlikome 212 kibernetinio saugumo subjektų[4] apklausą. Bendravome su Valstybinės duomenų apsaugos inspekcijos, Ryšių reguliavimo tarnybos, Informatikos ir ryšių departamento, Lietuvos kriminalinės policijos biuro, Kauno technologijos universiteto atstovais.

Audituojamasis laikotarpis – 2019–2021 m. Siekdami įvertinti tendencijas ir pokyčius, kai kuriais atvejais naudojome ankstesnių (2015–2018 m.) ir 2022 m. duomenis.

Auditas atliktas pagal tarptautinius aukščiausiųjų audito institucijų standartus. Audito apimtis ir taikyti metodai išsamiau aprašyti 2 priede „Audito apimtis ir metodai“ (43 psl.).

Pagrindiniai audito rezultatai

Tobulintina kibernetinio saugumo užtikrinimo sistema, nes: nacionaliniu lygiu neužtikrinamas tinkamas kibernetinio saugumo rizikos ir incidentų valdymas, nesudarytos tinkamos sąlygos vykdyti atitikties saugumo reikalavimams stebėseną, vis dar nekonsoliduotas kibernetinio saugumo ir elektroninės informacijos saugos teisinis reguliavimas, neužtikrinamas nuoseklus kibernetinio saugumo planavimo įgyvendinimas. Veiksmingai veikianti kibernetinio saugumo užtikrinimo sistema padidintų atsparumą kibernetinėms grėsmėms, efektyviai apsaugotų ypatingos svarbos informacinę infrastruktūrą, valstybės informacinius išteklius, sustiprintų atsaką kibernetinėms grėsmėms.

1. Saugumo valdymo sistema nepakankamai veiksminga

- Informacija apie kibernetinio saugumo subjektų identifikuotas kibernetinio saugumo rizikas nekaupiama bei nacionaliniu lygiu nevaldoma. Daugiau kaip trečdalis (38 proc., 81 iš 212) apklaustų kibernetinio saugumo subjektų neatlieka kibernetinio saugumo rizikos vertinimo, dėl to gali būti nepastebėtos naujos ar besikartojančios grėsmės, darančios įtaką subjektų saugos būklei ir jų veiklai. Kibernetinio saugumo rizikos vertinimo procesas reikalauja specifinių šios srities žinių ir įstaigų rizikos vertinimą atliekantys specialistai kokybiškai įvertinti kibernetinio saugumo rizikų negali, todėl tikslinga turėti rizikos vertinimo gaires. Daugiau nei pusė (56 proc., 74 iš 131) vertinimus atlikusių kibernetinio saugumo subjektų informacijos apie identifikuotas kibernetinio saugumo rizikas Nacionaliniam kibernetinio saugumo centrui nepateikia. Teisės aktuose neįtvirtinta prievolė kibernetinio saugumo subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, periodiškai teikti

[2] Kibernetinio saugumo įstatymas, 4 str. 2 d.

[3] Ten pat, 4 str. 3 d., 8 str. 2 d.

[4] Valstybės informacinių išteklių valdytojai ir tvarkytojai, nurodyti http://www.registrai.lt/ tinklalapyje, ir ypatingos svarbos informacinės infrastruktūros valdytojai (žiūrėta 2022-08-18).

Nacionaliniam kibernetinio saugumo centrui ryšių ir informacinių sistemų rizikos vertinimo ataskaitas. Kadangi nėra identifikuotų nacionalinių kibernetinio saugumo rizikų, nėra sudarytas nacionalinių kibernetinio saugumo rizikos valdymo priemonių planas ir nenustatyta priimtina nacionalinė kibernetinio saugumo rizika, jos tolerancijos ribos, todėl nacionaliniu lygiu nėra koordinuojamas rizikos valdymo procesas, kuriuo būtų užtikrinamas reikiamų apsaugos, prevencijos ir atsako priemonių bei pajėgumų panaudojimas (1.1 poskyris, 13 psl.).

- 2019–2021 m. beveik pusė (45 proc., 80 iš 176) valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų nė karto neatliko informacinių technologijų saugos atitikties vertinimo ir taip neįsitikino savo informacijos saugumo valdymo sistemos būkle, kad, prireikus, laiku galėtų imtis veiksmų ją tobulinti. Kasmet informacinių technologijų saugos atitikties vertinimų skaičius auga, tačiau 2021 m. nepateikta net 81 proc. valstybės informacinių išteklių informacinių technologijų saugos atitikties vertinimo ataskaitų. Didelė dalis (41 proc., 39 iš 96) informacinių technologijų saugos atitikties vertinimus atlikusių valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų duomenų Valstybės informacinių išteklių atitikties informacijos saugos reikalavimams stebėsenos sistemai neteikė. Tai mažina galimybes centralizuotai valdyti informaciją apie informacinių technologijų saugos neatitiktis ir nacionaliniu lygiu užtikrinti reikalavimų laikymosi priežiūrą. Valstybės kontrolė 2018 m. nustatė trūkumų[5], nors rekomendacijos priemonė turėjo būti įgyvendinta iki 2019-06-01, tačiau problemos iki šios dienos nėra išspręstos, nes pagal esamą programinį kodą nėra galimybės atlikti Valstybės informacinių išteklių atitikties informacijos saugos reikalavimams stebėsenos sistemos funkcinio praplėtimo, todėl ilgus metus problemos, kurių nepavyksta išspręsti, neigiamai veikia šį tvarumą, sudaro sąlygas pažeidžiamumams atsirasti (1.2 poskyris, 15 psl.).
- Krašto apsaugos ministerijai 2015 m. perėmus kibernetinio saugumo ir 2018 m. valstybės informacinių išteklių (elektroninės informacijos saugos) politikos formavimo funkcijas nebuvo konsoliduota šių sričių teisinė bazė. Valstybės kontrolė 2015 m. pateikė rekomendaciją[6] peržiūrėti ir suderinti (konsoliduoti) kibernetinio saugumo ir elektroninės informacijos saugos reikalavimus. Krašto apsaugos ir Vidaus reikalų ministerijos ją įsipareigojo įgyvendinti iki 2016 m. IV ketv., tačiau iki šiol vieningos saugumo reikalavimų sistemos projektas neparengtas. Tam tikri skirtinguose teisės aktuose išdėstyti reikalavimai kibernetiniam saugumui ir elektroninės informacijos saugai užtikrinti yra tapatūs, o tai apsunkina saugumo reikalavimų įgyvendinimą kibernetinio saugumo subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius (1.3 poskyris, 17 psl.).

2. Tobulintinas kibernetinių incidentų valdymas

- Kibernetinius incidentus valdančios ir (ar) tiriančios institucijos (Nacionalinis kibernetinio saugumo centras, Valstybinė duomenų apsaugos inspekcija, Lietuvos policija) ne visais atvejais keičiasi informacija apie kibernetinius incidentus, kurie joms aktualūs pagal jų veiklos pobūdį, todėl šios institucijos nesudaro prielaidų greitai atpažinti skirtingo pobūdžio kibernetinius incidentus ir perduoti kompetentingoms institucijoms informaciją, kad pastarosios galėtų laiku atlikti

[5] Valstybės informacinių išteklių atitikties informacijos saugos reikalavimams stebėsenos sistema sukurta valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenai palengvinti ir jos funkcionalumas nėra pakankamai panaudojamas.

[6] Prieiga per internetą: https://www.valstybeskontrole.lt/LT/Product/23587/kibernetinio-saugumo-aplinka-lietuvoje (žiūrėta 2022-08-18).

nusikalstamų veikų ar pažeidimų užkardymą, dėl to gali nukentėti kibernetinio saugumo subjektai ir visuomenė. Kibernetinio saugumo subjektai ir kibernetinius incidentus valdančios ir (ar) tiriančios institucijos informaciją apie kibernetinius incidentus turi perduoti per Kibernetinio saugumo informacinį tinklą, o jeigu tokios galimybės nėra, kitomis saugiomis informacijos perdavimo priemonėmis, tačiau Nacionalinis kibernetinio saugumo centras informaciją apie kibernetinius incidentus iš subjektų ir institucijų priima tik kitomis saugiomis informacijos perdavimo priemonėmis, bet ne per tinklą. Nustatėme, kad kibernetinio saugumo subjektai pasyviai naudojasi tinklu (per pastaruosius 3 mėn. 59 proc., arba 125 iš 212 subjektų nesinaudojo tinklu), o suinteresuotų šalių nuomone (Informatikos ir ryšių departamento, Ryšių reguliavimo tarnybos, Valstybinės duomenų apsaugos inspekcijos, Krašto apsaugos ministerijos), tinklas šiuo metu veikia neefektyviai ir galėtų būti plačiau pritaikytas naudojimui (2.1 poskyris, 21 psl.).

- Kibernetinio saugumo pratybos, mokymai ir konsultacijos kibernetinio saugumo klausimais vykdomos, bet yra nepakankamai rezultatyvios siekiant stiprinti kibernetinio saugumo subjektų gebėjimus efektyviai atremti kibernetines atakas ir užkirsti joms kelią. Kasmet rengiamos nacionalinės kibernetinio saugumo pratybos, organizuojami kibernetinio saugumo mokymai, teikiamos konsultacijos ir metodinės rekomendacijos, dauguma (73 proc., arba 101 iš 138 pratybose ir 72 proc., arba 73 iš 102 mokymuose dalyvavusiųjų) kibernetinio saugumo subjektų teigiamai jas vertina, tačiau kibernetinio saugumo subjektų įsitraukimas į pratybas ir mokymus yra nepakankamas: per tris pastaruosius metus (2019–2021 m.) net 35 proc. (74 iš 212) subjektų nė karto nedalyvavo pratybose, 52 proc. (110 iš 212) – mokymuose. Kas ketvirtas kibernetinio saugumo subjektas (26 proc., 55 iš 212) neturi kibernetinių incidentų valdymo plano (tvarkos), nėra patvirtintas tipinis kibernetinių incidentų valdymo planas, kuris turėtų būti pavyzdžiu kibernetinio saugumo subjektams. Jei šiems subjektams būtų nustatyta prievolė reguliariai dalyvauti kibernetinio saugumo pratybose ar mokymuose, patvirtintas tipinis kibernetinių incidentų valdymo planas, būtų užtikrintas šių subjektų kibernetinio saugumo kompetencijų ir įgūdžių stiprinimas, jie žinotų veiksmus, kurių reikia imtis įvykus kibernetiniam incidentui, veiksmingai jį suvaldyti ir užkirsti kelią galimoms grėsmėms (2.2 poskyris, 23 psl.).

3. Neužtikrinamas nuoseklus kibernetinio saugumo planavimo įgyvendinimas

- Nacionalinės kibernetinio saugumo strategijos įgyvendinimo stebėsena ir kontrolė orientuota į nuolatinį atsiskaitymą už pasiektą pažangą, tačiau 2019–2021 m. strategijos įgyvendinimo rezultatai nebuvo peržiūrimi kasmet: nuo 2021 m. įsigaliojus Strateginio valdymo įstatymui, Krašto apsaugos ministerija nerinko ir nesistemino informacijos apie Nacionalinės kibernetinio saugumo strategijos įgyvendinimo rezultatus, Strategijos vykdytojai stebėjo ne visas priemones ir vertinimo kriterijus. Iš 28 Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstituciniame veiklos plane numatytų priemonių tik 17 buvo visiškai įgyvendintos, 4 – neįgyvendintos, 7 – vykdytos, bet dėl COVID-19 pandemijos ir neįvykusių viešųjų pirkimų procedūrų buvo įgyvendintos ne visa apimtimi arba dėl baigtos priemonių įgyvendinimo stebėsenos nežinoma jų įgyvendinimo būklė. Dėl tų pačių priežasčių 11 (iš 38) strateginių rodiklių reikšmės nėra pasiektos, 5 (iš 38) – reikšmė nežinoma. 2020 m. buvo rengiamas Tarpinstitucinio veiklos plano pakeitimo projektas, tačiau dėl neatitikties Strateginio valdymo įstatymo normoms jis buvo sustabdytas. Nenuoseklus suplanuotų kibernetinio saugumo stiprinimo priemonių įgyvendinimas ir nepakankama stebėsena

lėmė tai, kad nacionalinių kibernetinio saugumo planavimo dokumentų nustatyti tikslai ir uždaviniai stiprinant valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą, skatinant kibernetinio saugumo kultūrą ir inovacijų plėtrą, nėra visiškai pasiekti vertinant 2021 m. Nacionalinės kibernetinio saugumo strategijos įgyvendinimo rezultatus pagal numatytus vertinimo kriterijus. Pažymėtina, kad strateginiame planavime numatyti pokyčiai – iki 2022 IV ketv. Krašto apsaugos ministerija turi parengti Nacionalinę kibernetinio saugumo plėtros programą, kuri apibrėžtų naujas pažangos (kibernetinio saugumo stiprinimo) priemones (3 skyrius, 28 psl.).

Rekomendacijos

Krašto apsaugos ministerijai

1. Siekiant užtikrinti kibernetinės apsaugos, prevencijos ir atsako priemonių panaudojimą, turi būti diegiamas ir nacionaliniu mastu koordinuojamas informacinių technologijų saugumo rizikų (įskaitant kibernetines) valdymo procesas, kuris leistų gautą informaciją apie kibernetinio saugumo rizikingumo būklę naudoti priimant strateginius sprendimus dėl kibernetinio saugumo stiprinimo (1-asis pagrindinis audito rezultatas).

2. Siekiant kibernetinio saugumo subjektams efektyviau įgyvendinti teisės aktuose nustatytus saugumo reikalavimus, sukurti bendrą valstybės informacinių išteklių kibernetinio saugumo ir informacinių technologijų saugos atitikties vertinimo metodiką, sudarančią galimybes atlikti išsamų atitikties teisės aktuose nustatytiems reikalavimams vertinimą, leisiančią priežiūrą ir stebėseną atliekančiai institucijai rezultatyviau pateikti duomenimis grįstą faktinės būklės nacionalinio lygiu analizę, įžvalgas, apibendrinimą (1-asis pagrindinis audito rezultatas).

3. Siekiant sudaryti sąlygas, kad visi kibernetinio saugumo subjektai žinotų veiksmus, kurių reikia imtis įvykus kibernetiniam incidentui ar siekiant užkirsti kelią galimoms grėsmėms:

   - patvirtinti priemones, kurios užtikrintų sklandesnį komunikavimą apie kibernetinius incidentus naudojantis kibernetinio saugumo informaciniu tinklu;
   - įpareigoti kibernetinio saugumo subjektus (valstybės informacinių išteklių valdytojus ir tvarkytojus, ypatingos svarbos informacinės infrastruktūros valdytojus) dalyvauti nacionalinėse kibernetinio saugumo pratybose ir numatyti Nacionalinio kibernetinio saugumo centro vykdomos švietimo veiklos vertinimo rodiklius bei periodiškai juos stebėti;
   - parengti ir patvirtinti detalų tipinį kibernetinių incidentų valdymo planą ir įpareigoti kibernetinio saugumo subjektus, pagal šio standartinio plano pavyzdį, parengti ar atnaujinti savo vidinius kibernetinių incidentų valdymo planus / tvarkas (2-asis pagrindinis audito rezultatas).

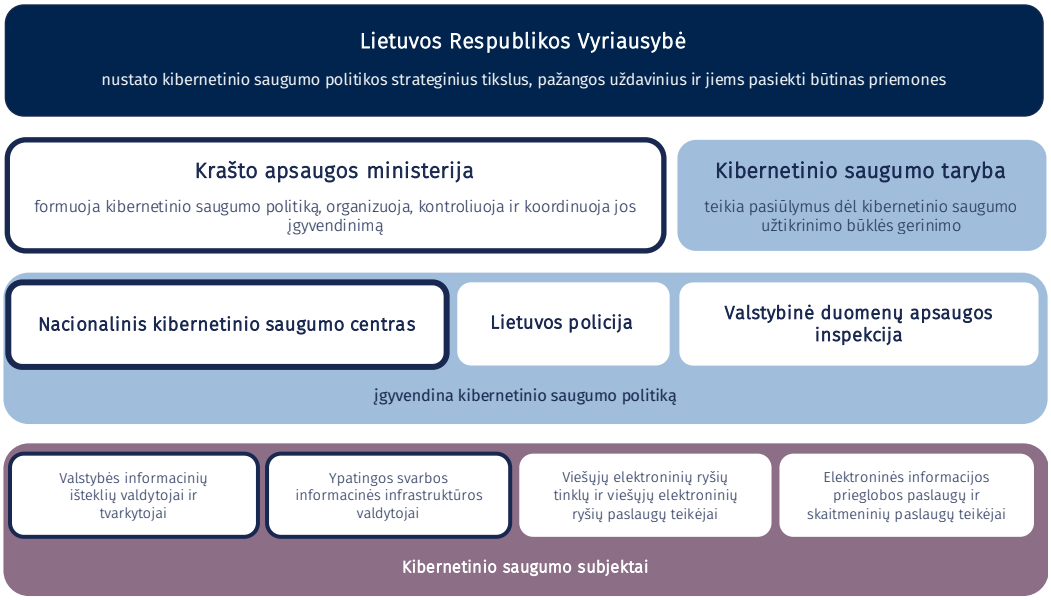
Rekomendacijų įgyvendinimo priemonės ir terminai, laukiamas audito poveikis ir pokyčių vertinimo rodikliai pateikti ataskaitos dalyje „Rekomendacijų įgyvendinimo planas“ (34 psl.). Aktuali informacija apie rekomendacijų įgyvendinimo būklę, rezultatus ir įvykusius pokyčius yra skelbiama atviruose duomenyse Valstybės kontrolės interneto svetainėje https://www.valstybeskontrole.lt/LT/AtviriDuomenys.

ĮŽANGA

Lietuvoje kibernetinio saugumo principus, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijas, šių institucijų įgaliojimus, kibernetinio saugumo subjektų pareigas, tarpinstitucinį bendradarbiavimą, ryšių ir informacinių sistemų spragų paieškos, pranešimo apie jas ir kibernetinius incidentus pagrindus nuo 2015 m. reglamentuoja Kibernetinio saugumo įstatymas. Pagal šiame įstatyme įtvirtintą sampratą kibernetiniu saugumu yra laikoma 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[7].

Kibernetinio saugumo srities valdymą Lietuvoje atlieka Vyriausybė, srities politiką formuoja Krašto apsaugos ministerija, įgyvendina Nacionalinis kibernetinio saugumo centras, Lietuvos policija, Valstybinė duomenų apsaugos inspekcija ir kitos įgaliotos valstybės institucijos, kibernetinio saugumo subjektai atsako už jų valdomų ryšių ir informacinių sistemų ar teikiamų paslaugų kibernetinį saugumą, užtikrina jų atitiktį nustatytiems kibernetinio saugumo reikalavimams (1 pav.)[8].

1 pav. Kibernetinio saugumo sistemos dalyviai



Šaltinis – Valstybės kontrolė pagal Kibernetinio saugumo įstatymą

[7] Kibernetinio saugumo įstatymas, 2 str. 10 d.

[8] Ten pat, 2 str. 8 d., 4 str., 7 str. 1 d. ir 11 str. 1 d. 1 p.

Dėl diferencijuoto teisinio reglamentavimo[9] audito metu vertinome kibernetinio saugumo subjektus, valdančius ir (arba) tvarkančius valstybės informacinius išteklius ir valdančius ypatingos svarbos informacinę infrastruktūrą. 2022 m. Lietuvoje registruotas 151 valstybės informacinių išteklių valdytojas ir 175 šių išteklių tvarkytojai[10], nustatyti 64 ypatingos svarbos informacinės infrastruktūros valdytojai[11].

Nuo 2015 m., kai Krašto apsaugos ministerija perėmė kibernetinio saugumo ir 2018 m. valstybės informacinių išteklių (elektroninės informacijos saugos) politikos formavimo funkcijas, įvyko teigiamų pokyčių kibernetinio saugumo srityje: 2018 m. į nacionalinę teisę perkeltos Europos Parlamento ir Tarybos direktyvos dėl tinklų ir informacinių sistemų saugumo nuostatos, patvirtinta Nacionalinė kibernetinio saugumo strategija, Ypatingos svarbos informacinės infrastruktūros identifikavimo metodika, Nacionalinis kibernetinių incidentų valdymo planas, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo pakeitimai. Nuo 2019 m. pradėtos vykdyti Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstituciniame veiklos plane numatytos šio saugumo stiprinimo priemonės. 2021 m. įkurtas Regioninis kibernetinės gynybos centras, įteisinta savanoriško kibernetinių spragų ir incidentų atskleidimo tvarka.

Pagal Tarptautinės telekomunikacijų sąjungos[12] 2021 m. paskelbtus tarptautinio kibernetinio saugumo indekso rezultatus Lietuva priklauso stipriausiųjų kibernetinio saugumo srityje šalių dešimtukui: Lietuva tarp pasaulio valstybių užėmė 6, tarp Europos valstybių – 4 vietą[13]. Tarptautinis kibernetinio saugumo indeksas parodo, kad šalyje galioja palyginti gera kibernetinio saugumo teisinė bazė, bet indekso skaičiavimo metodika neapima realios šio saugumo būklės vertinimo, t. y., kaip valstybės institucijos, ypatingos svarbos informacinės infrastruktūros valdytojai ir kitos organizacijos realiai yra pasirengusios atremti kibernetines atakas ir užtikrinti valdomos informacinės infrastruktūros ir tvarkomų informacinių išteklių saugumą[14].

2019–2021 m. užregistruota ypač daug kibernetinių atakų prieš Lietuvos valdžios institucijas, ypatingos svarbos informacinę infrastruktūrą, valstybės informacinius išteklius ir jų pagrindu veikiančias skaitmenines paslaugas. Nacionalinio kibernetinio saugumo centro duomenimis[15], 2019 m. buvo užfiksuotas 3 241 kibernetinis incidentas, 2020 m. – 4 330, 2021 m. – 4 088, iš viso 11 659 incidentai per tris metus.

Kibernetinis saugumas glaudžiai susijęs su elektroninės informacijos sauga, t. y. elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimu[16]. Veiksmingas kibernetinio saugumo ir elektroninės informacijos saugos užtikrinimas priklauso nuo teisingo

[9] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtintas Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas.

[10] Prieiga per internetą: https://registrai.lt/ (žiūrėta 2022-08-18).

[11] Vyriausybės 2021-03-08 nutarimu Nr. 145-2 patvirtintas Ypatingos svarbos informacinės infrastruktūros valdytojų sąrašas (su 2022-02-02 pakeitimais).

[12] International Telecommunication Union (ITU).

[13] Prieiga per internetą: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (žiūrėta 2022-06-22).

[14] Prieiga per internetą: https://www.mruni.eu/news/lietuva-pasaulinio-kibernetinio-saugumo-reitingo-desimtuke-kas-slepiasi-po-siuo-reitingu/ (žiūrėta 2022-06-22).

[15] Prieiga per internetą: https://www.nksc.lt/aktualu.html (Nacionalinio kibernetinio saugumo būklės ataskaitos, žiūrėta 2022-07-08).

[16] Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, 4.2 pp.

atitinkamų saugumo principų ir metodų nustatymo ir tinkamo valdymo procesų organizavimo. Tam tikros tarptautinės organizacijos ir asociacijos, pavyzdžiui: ISO[17], IEC[18], ISACA[19] ir kt., buvo įsteigtos tam, kad nustatytų standartizuotas taisykles ir procedūras, taikytinas projektuojant saugią IT infrastruktūrą, užtikrinant minimalų jos saugumą. ISO/IEC 27001 yra pagrindinis tarptautinis standartas, apibrėžiantis informacijos saugumo valdymo sistemos reikalavimus[20].

2018 m. patvirtinta Nacionalinė kibernetinio saugumo strategija penkerių metų laikotarpiui nustato svarbiausias nacionalinės kibernetinio saugumo politikos viešajame ir privačiame sektoriuose kryptis, tikslus, uždavinius[21]. Jos tikslų pasiekimas vertinamas pagal įgyvendinimo vertinimo kriterijus ir siekiamas jų reikšmes 2021 ir 2023 m.[22] bei Tarpinstituciniame veiklos plane nustatytas vertinimo kriterijų reikšmes 2019, 2020 ir 2021 m.[23] Teisės aktų nustatyta tvarka turi būti atliekami metiniai ir galutinis strategijos įgyvendinimo vertinimai[24].

[17] Tarptautinė standartizacijos organizacija.

[18] Tarptautinė elektrotechnikos komisija.

[19] Tarptautinė informacinių sistemų audito ir kontrolės asociacija.

[20] Prieiga per internetą: https://www.iso.org/isoiec-27001-information-security.html (žiūrėta 2022-07-20).

[21] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtinta Nacionalinė kibernetinio saugumo strategija, 1 p.

[22] Ten pat, 46 p., priedas.

[23] Vyriausybės 2019-07-03 nutarimu Nr. 709 patvirtintas Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas, 2 priedas.

[24] Nacionalinė kibernetinio saugumo strategija, 46, 49, 50 p.

AUDITO REZULTATAI

1. SAUGUMO VALDYMO SISTEMA NEPAKANKAMAI VEIKSMINGA

1. Valdant saugą, geroji praktika rekomenduoja įdiegti, valdyti ir stebėti informacijos saugumo valdymo sistemą[25], kuri saugo informacijos konfidencialumą, vientisumą ir prieinamumą, taikydama rizikos valdymo procesą ir užtikrina suinteresuotąsias šalis, kad rizikos yra tinkamai valdomos[26]. Tai reiškia, kad saugumo valdymas pagrįstas rizikos valdymu, kurio tikslas yra pasiekti priimtiną rizikos lygį, taip apsaugant informaciją, informacinę infrastruktūrą, ryšius ir informacinius išteklius nuo galimo tyčinio ir atsitiktinio poveikio.

1.1. Tobulintinas nacionalinis kibernetinio saugumo rizikos valdymas

2. Tam, kad nacionalinis kibernetinio saugumo rizikos valdymas būtų rezultatyvus, rekomenduojama apibrėžti suderintą rizikos valdymo metodiką, kurios laikytųsi visi kibernetinio saugumo subjektai, o jų atliktų rizikos vertinimų rezultatus teikti ir kaupti nacionaliniame rizikos registre. Tais atvejais, kai atliekamas decentralizuotas nacionalinio lygmens kibernetinio saugumo rizikos vertinimas ir kibernetinio saugumo subjektams yra palikta galimybė patiems pasirinkti rizikos vertinimo metodus, vertinimų rezultatai turėtų būti įtraukiami į nacionalinio lygmens rizikos valdymą[27].

3. Laikėmės nuostatos, kad kibernetinio saugumo rizikos valdymas nacionaliniu lygiu yra rezultatyvus, jeigu:

   - kaupiama informacija apie visų valstybės institucijų identifikuotas kibernetinio saugumo rizikas[28];
   - identifikuojamos ir analizuojamos kibernetinio saugumo rizikos[29];
   - suformuotas kibernetinio saugumo rizikos profilis[30];
   - parengta Nacionalinė kibernetinio saugumo rizikos vertinimo ataskaita[31];
   - patvirtintas Nacionalinis rizikos valdymo priemonių planas[32].

4. Subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, bei ypatingos svarbos informacinės infrastruktūros valdytojams teisės aktuose numatyta prievolė

[25] Cobit®5: Enabling Processes, APO13 proceso „Valdyti saugą“ aprašymas, 113-115 psl.

[26] LST EN ISO/IEC 27001:2017 Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai, 7 psl.

[27] ITU Guide to Developing a National Cybersecurity Strategy, 2018, 5.2.1 pp.

[28] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtinta Nacionalinė kibernetinio saugumo strategija, 14.1 pp., ITU Guide to Developing a National Cybersecurity Strategy, 2018, 5.2.1 pp.

[29] Nacionalinė kibernetinio saugumo strategija, 14.1 pp., ENISA National-level Risk Assessments, 2013, 3.2.5, 4.1 pp., Cobit®5: Enabling Processes, APO12 „Valdyti riziką“ proceso aprašymas, 107–111 psl.

[30] ITU Guide to Developing a National Cybersecurity Strategy, 2018, 5.2.3 pp., Procesų vertinimo modelis, naudojant COBIT®5, APO12 proceso „Valdyti riziką“ BP3 bazinės praktikos „Valdyti rizikos profilį“ aprašymas, 61 psl.

[31] ITU Guide to Developing a National Cybersecurity Strategy, 2018, 5.2.1 pp.

[32] Ten pat.

ne rečiau kaip kartą per metus arba po esminių organizacinių ar sisteminių pokyčių organizuoti ir atlikti ryšių ir informacinių sistemų rizikos vertinimą[33]. Nustatėme, kad per 3 metus (2019–2021 m.) 38 proc. (81 iš 212) auditorių apklaustų kibernetinio saugumo subjektų nė karto neatliko kibernetinio saugumo rizikos vertinimo, o didelė dalis (56 proc., arba 74 iš 131) vertinimus atlikusiųjų informacijos apie identifikuotas kibernetinio saugumo rizikas NKSC nepateikė. Informacija apie valstybės institucijų identifikuotas kibernetinio saugumo rizikas nėra kaupiama, pagal teisės aktų reikalavimus visi kibernetinio saugumo subjektai turi atlikti ryšių ir informacinių sistemų rizikos vertinimą, tačiau teisės aktuose rizikos vertinimo rezultatų periodinio pateikimo atsakingoms valstybės institucijoms prievolė nenustatyta[34].

5. Kibernetinio saugumo rizikos vertinimo procesas reikalauja specifinių šios srities žinių ir įstaigų rizikos vertinimą atliekantys specialistai kokybiškai įvertinti kibernetinio saugumo rizikų negali, todėl tikslinga turėti rizikos vertinimo gaires. Nacionaliniu mastu nėra nurodyta, kokią konkrečią rizikos vertinimo metodiką kibernetinio saugumo subjektai turi naudoti: Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše tik rekomenduojama vadovautis Lietuvos ir tarptautiniais standartais ar metodikomis, reglamentuojančiais rizikos valdymą[35], o Bendrųjų elektroninės informacijos saugos reikalavimų apraše siūloma atsižvelgti į metodinę priemonę „Rizikos analizės vadovas“[36], Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus“[37].

6. Geroji praktika rekomenduoja[38] sudaryti sektorinius rizikos profilius, kuriuose būtų pateikta kiekybinė esamų grėsmių tipų analizė, ir periodiškai juos atnaujinti. Nustatėme, kad nacionalinio kibernetinio saugumo rizikos profilis nėra suformuotas.

7. NKSC teigimu, nacionalinis kibernetinių saugumo rizikos vertinimas ir analizė pateikiami kasmetinėse kibernetinio saugumo būklės ataskaitose[39] bei Priešgaisrinės apsaugos ir gelbėjimo departamento atliekamoje Nacionalinėje rizikos analizės ataskaitoje[40]. Atlikę dokumentų peržiūrą nustatėme, kad NKSC kasmetinėse ataskaitose apžvelgiama kibernetinių incidentų, bet ne kibernetinio saugumo rizikų situacija, o nacionalinės rizikos analizės ataskaitos „Kibernetinės atakos“ skyriuje nepateikiama išsami nacionalinio kibernetinio saugumo rizikos analizė. Kadangi šios rizikos neidentifikuotos, nėra

[33] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtintas Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, 5.1 pp.

[34] Išskyrus atvejus, kai valstybės informacinių išteklių valdytojai/tvarkytojai rizikos vertinimą atlieka kartu su Valstybės informacinių išteklių rizikos arba IT saugos atitikties vertinimu ir duomenis į ARSIS pateikia Bendrųjų elektroninės informacijos saugos reikalavimų aprašo 38 ir 45 p. nustatyta tvarka.

[35] Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, 4 p.

[36] Prieiga per internetą: https://www.nksc.lt/doc/rizikos_analize.pdf (žiūrėta 2022-07-25). Pažymėtina, kad vadovą parengė VRM 2005 m. NKSC teigimu, jis atitinka šiuolaikinių rizikų vertinimo metodikas, nes parengtas vadovaujantis gerosiomis praktikomis. KAM nurodė, kad šiuo metu vadovo atnaujinti nenumatyta.

[37] Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, 35 p.

[38] Procesų vertinimo modelis, naudojant COBIT®5, APO12 proceso „Valdyti riziką“ BP3 bazinės praktikos „Valdyti rizikos profilį“ aprašymas, 61–62 psl., ITU Guide to Developing a National Cybersecurity Strategy, 2018, 5.2.3 pp.

[39] Prieiga per internetą: https://www.nksc.lt/aktualu.html (Aktuali informacija, reglamentavimas, statistika | NKSC) (žiūrėta 2022-07-25).

[40] Prieiga per internetą: https://pagd.lrv.lt/lt/veiklos-sritys-1/civiline-sauga/nacionaline-rizikos-analize (žiūrėta 2022-07-25).

sudarytas nacionalinės kibernetinių rizikos valdymo priemonių planas ir nenustatyta priimtina nacionalinė kibernetinio saugumo rizika, jos tolerancijos ribos[41].

8. Nacionalinio kibernetinio saugumo rizikos vertinimo metu gauta informacija turi būti naudojama, priimant strateginius sprendimus kibernetinio saugumo srityje, siekiant užtikrinti priimtiną rizikos lygį, todėl reikėtų gerinti kibernetinio saugumo rizikos valdymą, diegti nacionalinį valdymo procesą. Toks rizikos valdymas leistų atitinkamoms institucijoms (KAM, NKSC) gauti politikos formavimui aktualią informaciją apie kibernetinio saugumo subjektų identifikuotas rizikas ir nacionaliniu lygiu koordinuoti jų valdymo procesą, kuriuo būtų užtikrinamas reikiamų apsaugos, prevencijos, atsako priemonių ir pajėgumų panaudojimas.

1.2. Nesudarytos sąlygos skaitmenizuotai vykdyti saugumo reikalavimų atitiktį ir stebėseną

9. Siekiant strateginių tikslų, kiekviena organizacija turi stebėti, vertinti ir įvertinti veiklos efektyvumą ir atitiktį, žinoti savo IT valdymo būklę, užtikrinti nuolatinę jo stebėseną[42]. Efektyviai organizuota stebėsena parodo atitinkamo laikotarpio pažangos pokytį, identifikuoja spręstinas strategines problemas. Atliekant IT stebėseną ir vertinimą, reikėtų nustatyti tinkamus veiklos efektyvumo vertinimo kriterijus, sistemingai atlikti IT valdymo būklės vertinimus ir vadovaujantis gautais rezultatais nustatyti tobulinimo veiksmus. Viena iš IT valdymo sričių yra saugumas, kurio stebėsenai nuo 2016 m. sukurta ARSIS.

10. ARSIS tikslas – IT priemonėmis atlikti valstybės informacinių išteklių atitikties teisės aktų nustatytiems elektroninės informacijos saugos reikalavimams stebėseną. ARSIS uždavinys: automatizuoti duomenų apie saugos reikalavimų įgyvendinimą informaciniuose ištekliuose tvarkymo, valstybės ir kitų IS, valstybės ir žinybinių registrų rizikos vertinimo, atitikties saugos reikalavimams priežiūros, IS ir registrų valdytojų informavimo apie jų valdomiems informaciniams ištekliams taikomus saugos reikalavimus ir elektroninės informacijos saugos rizikas procesus[43].

11. Laikėmės nuostatos, kad atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistema užtikrina atitikties teisės aktų nustatytiems kibernetinio saugumo reikalavimams vertinimą, jeigu:

    - 100 proc. atrinktų valstybės informacinių sistemų, valstybės ir žinybinių registrų valdytojų ir (ar) tvarkytojų atlieka ir teikia atitikties vertinimus ARSIS[44];
    - ARSIS sudaryta galimybė atlikti atitikties kibernetinio saugumo reikalavimams vertinimą[45];
    - NKSC pagal atliktus vertinimus atlieka stebėseną[46].

[41] Procesų vertinimo modelis, naudojant COBIT®5, EDM03 „Užtikrinti rizikos optimizavimą“ proceso aprašymas, 23 psl.

[42] Procesų vertinimo modelis, naudojant COBIT®5, MEA01 proceso „Stebėti, vertinti ir įvertinti veiklos efektyvumą ir atitiktį“ aprašymas, 107-108 psl.

[43] Krašto apsaugos ministro 2018-12-11 įsakymu Nr. V-1183 patvirtinti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatai, 3 ir 4 p.

[44] Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, 2, 44 ir 45 p., Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatai, 48 p.

[45] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtinta Nacionalinė kibernetinio saugumo strategija, 14.1 pp.

[46] Kibernetinio saugumo įstatymas, 8 str. 2 d. 1 p., krašto apsaugos ministro 2013-12-31 įsakymu Nr. V-1200 patvirtinti Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos nuostatai, 9.4 pp.

12. ARSIS duomenų teikėjai yra kibernetinio saugumo subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius[47]. Vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu[48], atlikus IT saugos atitikties vertinimą, rengiama vertinimo ataskaita. Šie subjektai[49] turi IT saugos atitikties vertinimo ataskaitą ir pastebėtų trūkumų šalinimo planą teikti į ARSIS[50]. Nustatėme, kad per 3 metus (2019–2021 m.) 46 proc. (80 iš 176) audito metu apklaustų valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų nė karto neatliko IT saugos atitikties vertinimo ir taip nesudarė sąlygų vertinti savo saugos valdymo sistemos ir, esant poreikiui, imtis veiksmų ją tobulinti.

Valstybės informacinių išteklių valdytojų ir tvarkytojų nurodytos priežastys, kodėl neatliekami IT saugos atitikties vertinimai

- žmogiškųjų išteklių trūkumas;
- finansavimo nepakankamumas;
- kompetencijos trūkumas;
- vertinimus tik planuojama atlikti;
- atliekamas atitikties kibernetinio saugumo reikalavimams vertinimas.

13. Atlikę NKSC pateiktos informacijos analizę nustatėme, kad kasmet valstybės informacinių išteklių, kurių IT saugos atitikties ataskaitos pateiktos, skaičius auga, bet 2021 m. nepateiktos net 81 proc. (327 iš 403[51]) jų IT saugos atitikties vertinimo ataskaitos (1 lentelė).

1 lentelė. IT saugos atitikties vertinimo ataskaitų (vnt.) pateikimas Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai

	2019 m.	2020 m.	2021 m.
Ataskaitas pateikusių valdytojų ir (arba) tvarkytojų skaičius	24	21	36
Valstybės informacinių išteklių, kurių ataskaitos pateiktos, skaičius	36	63	76

Šaltinis – Valstybės kontrolė pagal NKSC pateiktą informaciją

Taip pat nustatėme, kad 41 proc., arba 39 iš 96, IT saugos atitikties vertinimus atlikusių valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų duomenų į ARSIS neteikė. Informacijos nepateikus, nesudaroma galimybių centralizuotai valdyti informaciją apie neatitiktis nacionaliniu lygiu ir užtikrinti reikalavimų laikymosi priežiūrą.

Informacinių išteklių valdytojų/ tvarkytojų nurodytos priežastys dėl IT saugos atitikties vertinimų ataskaitų nepateikimo į ARSIS

- sudėtinga sistema;
- neturi prisijungimų;
- planuojama pateikti;
- medžiaga teikta NKSC;
- nenustatyta kritinių rizikų.

[47] Krašto apsaugos ministro 2018-12-11 įsakymu Nr. V-1183 patvirtinti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatai, 15.2 pp.

[48] Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, VII sk.

[49] Valstybės informacinių išteklių valdytojai ir (arba) tvarkytojai.

[50] Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, 2, 44 ir 45 p., Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatai, 48 p.

[51] Remiantis www.registrai.lt duomenimis, iš viso yra 403 valstybės informaciniai ištekliai: 308 valstybės informacinės sistemos ir 95 valstybės registrai (žiūrėta 2022-06-06).

14. Valstybės informacinių išteklių valdytojams ir (arba) tvarkytojams bei ypatingos svarbos informacinės infrastruktūros valdytojams teisės aktuose yra numatytas reikalavimas ne rečiau kaip kartą per metus organizuoti ir atlikti valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimą[52], tačiau nėra sudarytos galimybės vertinimo atlikti naudojantis ARSIS. Nenustatyta šių vertinimų duomenų teikimo į ARSIS tvarka.

15. NKSC turi atlikti informacinių išteklių ir kibernetinio saugumo subjektų atitikties teisės aktų nustatytiems kibernetinio saugumo ir elektroninės informacijos saugos reikalavimams vertinimą, priežiūrą ir stebėseną[53]. ARSIS yra sudaryta galimybė atlikti valstybės informacinių išteklių atitikties teisės aktų nustatytiems elektroninės informacijos saugos reikalavimams vertinimą, tačiau pagal 2022-05-26 ARSIS funkcionalumą nėra galimybės vertinti atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams.

16. Kibernetinio saugumo subjektų teigimu, ARSIS yra neefektyvi, nepalaikoma, nesuteikianti grįžtamojo ryšio. Sistema svarbi sukauptos informacijos prasme, tačiau joje nėra apibendrinimo, vertinimo rodiklių, įžvalgų. Subjektai nurodė, kad ARSIS tėra popierinių dokumentų archyvas, nors sistema turėtų būti įrankis, kuris padėtų matyti bendrą vaizdą, pasilyginti su kitais. Valstybės kontrolė 2018 m. teikė rekomendacijas, nes buvo nustatytos problemos, jog sistema sukurta tik saugos atitikties stebėsenai palengvinti ir jos funkcionalumas nėra pakankamai panaudojamas. Rekomendacijos priemonė turėjo būti įgyvendinta iki 2019-06-01, tačiau problemos iki šios dienos nėra išspręstos, nes pagal esamą programinį kodą nėra galimybės atlikti ARSIS funkcijų praplėtimo.

17. ARSIS, kaip saugumo reikalavimų atitikties vertinimo ir stebėsenos įrankis, yra svarbus elementas užtikrinant kibernetinio saugumo sistemos tvarumą, todėl nuo 2018 m. problemos, kurių nepavyksta išspręsti, neigiamai veikia šį tvarumą, sudaro sąlygas atsirasti pažeidžiamumams.

18. Atitikties teisės aktų nustatytiems saugos reikalavimams priežiūros ir stebėsenos metu gauta informacija turėtų būti naudojama grįžtamajam ryšiui suteikti, kuris palengvintų kibernetinio saugumo subjektams įgyvendinti šiuos reikalavimus. Svarbu sukurti bendrą kibernetinio saugumo ir informacinių išteklių saugos atitikties vertinimo metodiką, sudarančią galimybes atlikti išsamų atitikties teisės aktuose nustatytiems reikalavimams vertinimą ir padėtų priežiūrą bei stebėseną atliekančiai institucijai pateikti nacionalinio lygmens faktinės būklės analizę, įžvalgas, apibendrinimą.

1.3. Dar nėra konsoliduotas kibernetinio saugumo ir elektroninės informacijos saugos teisinis reguliavimas

19. Geroji IT valdymo praktika rekomenduoja sukurti informacijos saugumo valdymo sistemą, kuri reglamentuotų saugumo principus, formalius ir nuolatinius informacijos saugos valdymo metodus[54], užtikrintų nustatytos politikos, principų, standartų, procedūrų, metodikų atitiktį

[52] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtintas Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, 9 p.

[53] Kibernetinio saugumo įstatymas, 8 str. 2 d. 1 p., krašto apsaugos ministro 2013-12-31 įsakymu Nr. V-1200 patvirtinti Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos nuostatai, 9.4 pp.

[54] Cobit®5: Enabling Processes, APO13 „Valdyti saugą“ proceso aprašymas, 113-115 psl.

visiems taikomiems tarptautiniams (išorės) reikalavimams[55]. Saugumo valdymo sistemos kūrimo, veikimo ir plėtros reikalavimus, kontrolės priemonių tikslus ir kontrolės priemones nustato tarptautinis informacijos saugumo valdymo standartas ISO 27001[56], atskiroms sritims ir sektoriams taikytinus saugumo reikalavimus – kiti ISO 27k standartai ir vadovai[57].

20. KAM, kaip kibernetinio saugumo ir valstybės informacinių išteklių (elektroninės informacijos) saugos srityje politikos formuotoja[58], rengia kibernetinio saugumo ir valstybės informacinių išteklių (elektroninės informacijos) saugos reikalavimus[59].

21. Laikėmės nuostatos, kad kibernetinio saugumo teisinis reguliavimas veiksmingas, jeigu:

    - visi kibernetinio saugumo reikalavimai nesidubliuoja su elektroninės informacijos saugos reikalavimais[60];
    - nustatyti organizaciniai ir techniniai kibernetinio saugumo reikalavimai atitinka tarptautines šios srities gerąsias praktikas[61].

22. Kibernetinio saugumo subjektų apklausa parodė, kad, 53 proc. (113 iš 212) apklaustųjų nuomone, kibernetinio saugumo ir elektroninės informacijos saugos reikalavimai nėra integralūs, nes reikalavimai ar dalis jų dubliuojasi.

23. Atlikę kibernetinio saugumo ir elektroninės informacijos saugos reikalavimų[62] sugretinimą nustatėme, kad šio saugumo reikalavimai yra tapatūs su elektroninės informacijos saugos reikalavimais (pavyzdys, ir žr. 4 priedą). Dėl tapačių, skirtinguose teisės aktuose išdėstytų reikalavimų kibernetiniam saugumui ir elektroninės informacijos saugai užtikrinti, kibernetinio saugumo subjektai, valdantys ir (ar) tvarkantys valstybės informacinius išteklius, patiria didesnę[63] administracinę naštą įgyvendinant saugumo reikalavimus.

Kibernetinio saugumo ir elektroninės informacijos saugos reikalavimų tapatumo pavyzdžiai

Reikalavimų sritis	Kibernetinio saugumo reikalavimai	Elektroninės informacijos saugos reikalavimai
Saugumo politikos peržiūra[64]	Kibernetinio saugumo politikos ir jos įgyvendinimo dokumentai turi būti peržiūrimi (persvarstomi) ne rečiau kaip kartą per metus. Keičiami kibernetinio saugumo	Saugos dokumentai institucijoje turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per metus informacinės sistemos valdytojo vadovo nustatyta tvarka. <...> Keičiami saugos dokumentai derinami su krašto apsaugos

[55] Cobit®5: Enabling Processes, MEA03 „Stebėti, vertinti ir įvertinti išorės reikalavimų laikymąsi“ proceso aprašymas, 213-215 psl.

[56] Prieiga per internetą: https://www.iso.org/isoiec-27001-information-security.html (žiūrėta 2022-07-20).

[57] Ten pat.

[58] Kibernetinio saugumo įstatymas, 4 str. 2 d., Valstybės informacinių išteklių valdymo įstatymas, 5 str. 4 d.

[59] Kibernetinio saugumo įstatymas, 6 str. 2 p., Valstybės informacinių išteklių valdymo įstatymas, 5 str. 4 d. 1 p.

[60] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtinta Nacionalinė kibernetinio saugumo strategija, 14.2 pp.

[61] Nacionalinė kibernetinio saugumo strategija, 14.2 pp., Cobit®5: Enabling Processes, MEA03 „Stebėti, vertinti ir įvertinti išorės reikalavimų laikymąsi“ proceso aprašymas, 213–215 psl.

[62] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtintas Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtinti Bendrųjų elektroninės informacijos saugos reikalavimų ir Saugos dokumentų turinio gairių aprašai, krašto apsaugos ministro 2020-12-04 įsakymu Nr. V-941 patvirtintas Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašas.

[63] Administracinės naštos mažinimo įstatymas, 3 str. 1 d. 1 p.

[64] LST EN ISO/IEC 27001:2017 Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai, A.5.1.2 pp.

	politikos ir jos įgyvendinimo dokumentai su Nacionaliniu kibernetinio saugumo centru gali būti nederinami tais atvejais, kai atliekami tik redakciniai pakeitimai. Tokiais atvejais Nacionaliniam kibernetinio saugumo centrui pateikiamos šių dokumentų kopijos[65].	ministro įgaliota institucija, įgyvendinančia valstybės informacinių išteklių saugos politiką[66], aprašo nustatyta tvarka. Keičiami saugos dokumentai gali būti su krašto apsaugos ministro įgaliota institucija, įgyvendinančia valstybės informacinių išteklių saugos politiką[67], nederinami tais atvejais, kai atliekami tik redakciniai ar nežymūs nustatyto teisinio reguliavimo esmės ar saugos politikos nekeičiantys pakeitimai arba taisoma teisės technika[68].
Kriptografinės kontrolės priemonių naudojimas[69]	Viešaisiais elektroninių ryšių tinklais perduodamos informacijos konfidencialumas turi būti užtikrintas naudojant šifravimą, virtualųjį privatų tinklą (angl. *Virtual private network*, VPN)[70].	Viešaisiais ryšių tinklais perduodamos informacinės sistemos elektroninės informacijos konfidencialumas turi būti užtikrintas, naudojant šifravimą, virtualų privatų tinklą (angl. *virtual private network*), skirtines linijas, saugų elektroninių ryšių tinklą ar kitas priemones)[71].

24. Kibernetinis saugumas glaudžiai susijęs su informacijos sauga, tačiau iki KAM perėmė koordinuoti valstybės informacinių išteklių saugos ir kibernetinio saugumo sritis[72], jų politikas formavo dvi institucijos – KAM ir VRM. 2015 m. atlikę valstybinį auditą „Kibernetinio saugumo aplinka Lietuvoje“, ministerijoms teikėme rekomendaciją iki 2016 m. IV ketv. peržiūrėti kibernetinio saugumo ir elektroninės informacijos saugos reikalavimus, juos suderinti ir (arba) patvirtinti trūkstamas nuostatas ir metodinius dokumentus[73], bet šie reikalavimai iki šiol reglamentuoti skirtinguose teisės aktuose[74]. 2020 m. KAM parengė pasiūlymą dėl naujos tarptautiniais standartais grįstos kibernetinio saugumo reikalavimų sistemos, kuri 2021-03-02 buvo pristatyta Kibernetinio saugumo tarybos posėdyje, bet vieningos organizacinių ir techninių saugumo reikalavimų struktūros ir nuostatų projektas rengiamas 7 metus.

25. VRM yra teikusi Vyriausybei siūlymą[75] konsoliduoti kibernetinio saugumo ir valstybės informacinių išteklių (elektroninės informacijos) saugos teisinį reglamentavimą, sujungti elektroninės informacijos saugą ir kibernetinį saugumą reglamentuojančių teisės aktų reikalavimus, kad būtų išvengta teisės normų dubliavimo, kolizijos ir konkurencijos atvejų,

[65] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtintas Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, 8 p.

[66] Nacionalinis kibernetinio saugumo centras – krašto apsaugos ministro įgaliota institucija, įgyvendinanti valstybės informacinių išteklių saugos politiką.

[67] Tas pat.

[68] Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, 13 p.

[69] LST EN ISO/IEC 27001:2017 Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai, A.10.1.1 pp.

[70] Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, priedo 4 p.

[71] Krašto apsaugos ministro 2020-12-04 įsakymu Nr. V-941 patvirtintas Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašas, 6.2 pp.

[72] Nuo 2018-01-01 įsigaliojo Valstybės informacinių išteklių valdymo įstatymo Nr. XI-1807 5, 6, 43 ir 43-1 straipsnių pakeitimo įstatymas, nuo 2015-01-01 – Kibernetinio saugumo įstatymas.

[73] Prieiga per internetą: https://www.valstybeskontrole.lt/LT/Product/Download/3358 (žiūrėta 2022-07-25).

[74] Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas ir Bendrųjų elektroninės informacijos saugos reikalavimų aprašas.

[75] 2021-06-07 raštas „Dėl registrų ir valstybės informacinių sistemų steigimo, kūrimo ar modernizavimo proceso tobulinimo“.

būtų išgrynintos teisės aktuose vartojamos sąvokos ir suformuluota aiški, tiksli ir optimali saugumo reikalavimų sistema.

26. KAM ir kitų atsakingų institucijų nuomone, teisinė bazė tobulintina, tikslinga peržiūrėti esamus reikalavimus.

Atsakingų institucijų nuomonė apie teisinį reglamentavimą

IRD: KAM perėmus koordinuoti informacinių išteklių saugos ir kibernetinio saugumo sritis nebuvo konsoliduota teisinė bazė. Šios dvi sritys yra atskirai reglamentuotos, tad atitinkamai – keliami ir atskiri reikalavimai. Toks skirstymas apsunkina įgyvendinančių įstaigų veiklą ir tampa neaiški jų atitiktis, pavyzdžiui, įstaiga atitinka informacinių išteklių reikalavimus, tačiau neatitinka kibernetinio saugumo reikalavimų, nors turėtų koreliuoti. Kyla dvejonė dėl galutinio rezultato, įvertinimo. Tikslinga apjungti šiuos reikalavimus įtraukiant tarptautinių standartų (NIST, ISO) reikalavimus. Teisinė bazė yra pasenusi, tad būtina peržvelgti taikomus reikalavimus.

VDAI: Sudėtinga dirbti, kai reikalavimus reikia „susirinkti“ iš skirtingų teisės aktų, nes nėra aiškumo, supratimo, vientisumo. Taip pat nustatytos teisės aktų nuostatos ne visais atvejais yra veiksmingos. Valdant saugą organizacijos turėtų nusistatyti organizacinius ir techninius reikalavimus pagal rizikų vertinimą, bet ne pagal aprašą.

KAM: Dabartiniai organizaciniai ir techniniai saugumo reikalavimai Lietuvoje yra nelankstūs. Būtų tikslinga pereiti prie kibernetinio saugumo reikalavimų taikymo įvairioms valdymo sritimis. Jei turėtume gerą saugumo valdymo modelį, neprireiktų tiek daug reikalavimų.

27. Atlikę kibernetinį saugumą ir elektroninės informacijos saugą reglamentuojančių teisės aktų palyginimą su ISO 27001 standarto[76] reikalavimais, nustatėme, kad saugumo valdymo politika ir saugos kontrolės priemonės parengti pagal šio standarto rekomendacijas.

28. Nustatyti organizaciniai ir techniniai saugumo valdymo reikalavimai[77] atitinka šios srities gerąsias praktikas[78], tačiau skirtinguose teisės aktuose nustatyti saugumo reikalavimai sudaro prielaidas didėti administracinei naštai kibernetinio saugumo subjektams (valstybės informacinių išteklių valdytojams ir tvarkytojams) ir sukelia neaiškumų juos taikant.

2. TOBULINTINAS KIBERNETINIŲ INCIDENTŲ VALDYMAS

29. ISACA ir CMMI instituto tyrimų duomenimis, stiprią kibernetinio saugumo kultūrą turinčios organizacijos turi geresnį suvokimą apie galimas grėsmes, mažesnį kibernetinių incidentų skaičių ir didesnį atsparumą galimoms grėsmėms[79]. Į naujausias kibernetinio saugumo tendencijas orientuotos ir reguliariai organizuojamos kibernetinio saugumo pratybos ir mokymai didina darbuotojų atidumą ir kibernetinio saugumo kultūrą[80].

[76] LST EN ISO/IEC 27001:2017 Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai.

[77] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtintas Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas; Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Bendrųjų elektroninės informacijos saugos reikalavimų aprašas; krašto apsaugos ministro 2020-12-04 įsakymu Nr. V-941 patvirtintas Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašas.

[78] LST EN ISO/IEC 27001:2017 Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai.

[79] Prieiga per internetą: https://www.isaca.org/-/media/info/cybersecurity-culture-report/index.html (žiūrėta 2022-06-29).

[80] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtinta Nacionalinė kibernetinio saugumo strategija, 25 p.

30. Kibernetiniai nusikaltėliai nuolat randa naujų būdų apeiti kibernetinio saugumo priemones. 2021 m. 94 proc. kenkėjiškų programų buvo pristatyta el. paštu[81], o 85 proc. duomenų pažeidimų buvo susiję su žmogiškuoju elementu[82].

2.1. Apie kibernetinius incidentus turi būti komunikuojama sklandžiau

31. Tam, kad komunikavimas apie kibernetinius incidentus būtų sklandus, geroji praktika rekomenduoja stiprinti CSIRT[83] ir teisėsaugos institucijų bendradarbiavimą, nes jų veikla glaudžiai susijusi su šių incidentų valdymu. Šių institucijų bendradarbiavimas ir dalijimasis turima informacija apie kibernetinių incidentų tendencijas ir grėsmes laikoma svarbia kibernetinio saugumo užtikrinimo priemone. Labai svarbus bendradarbiavimo veiksnys – tinkamas informacijos apsikeitimas reikiamu laiku. Įvykus incidentui, CSIRT turi patikrinti, ar yra nusikalstamos veikos požymių ir, vadovaujantis rekomendacijomis apie visus galimus elektroninius nusikaltimus, pranešti atitinkamoms teisėsaugos institucijoms[84].

32. Laikėmės nuostatos, kad komunikavimas apie kibernetinius incidentus yra sklandus, jeigu:

- 0 proc. atrinktųjų incidentų, apie kuriuos pranešta ne vieno langelio[85] principu tiesiogiai NKSC[86];
- 100 proc. atrinktų incidentų, apie kuriuos buvo pranešta LP ir VDAI, buvo pateikti NKSC; 100 proc. atrinktų incidentų, apie kuriuos buvo pranešta NKSC ir VDAI ir galėjo turėti nusikalstamos veikos požymių, buvo pateikti LP; 100 proc. atrinktų incidentų, apie kuriuos pranešta NKSC ir LP ir galėjo būti susiję su asmens duomenų saugumo pažeidimais, buvo pateikti VDAI[87];
- 100 proc. atrinktų kibernetinio saugumo subjektų, kurie per pastaruosius 3 mėn. naudojosi KSIT; 100 proc. atrinktų incidentų NKSC pateikta per KSIT; 100 proc. atrinktų incidentų, apie kuriuos buvo pranešta NKSC, LP ir VDAI, informacija perduota per KSIT[88].

33. KIVT institucija, gavusi informaciją apie kibernetinį incidentą, nedelsdama, bet ne vėliau kaip per 24 val. nuo informacijos apie incidentą gavimo informuoja kitas KIVT institucijas: NKSC (nustačiusi, kad incidentas gali paveikti kibernetinio saugumo subjektų ryšius ir informacines sistemas); LP (nustačiusi, kad incidentas gali turėti nusikalstamos veikos požymių); VDAI (nustačiusi, kad incidentas gali būti susijęs su asmens duomenų saugumo pažeidimais)[89]. Nustatėme, kad ne visos KIVT institucijos ne visais atvejais keičiasi informacija apie kibernetinius incidentus, kurie gali būti joms aktualūs:

- LP auditoriams nepateikė informacijos dėl gautos informacijos ar kreipimųsi tiesiogiai iš kibernetinio saugumo subjektų dėl kibernetinių incidentų, galimai turinčių

[81] El. laiškai siunčiami kaip teisėtas šaltinis, siekiant priversti aukas atskleisti neskelbtiną informaciją, pvz., slaptažodžius, asmens identifikavimo duomenis ar kitą konfidencialią informaciją.

[82] Prieiga per internetą: https://www.verizon.com/business/en-sg/resources/reports/dbir/ (žiūrėta 2022-06-29).

[83] Reagavimo į kompiuterinio saugumo incidentus tarnyba (angl. *Computer Security Incident Response Team*).

[84] ENISA Roadmap on the cooperation between CSIRTS and LE, 2019, 5.2.1 pp., ENISA Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime, 2012, 3.1.2, 4.2.5, 4.3, 7.2.10 pp.

[85] Prieiga per internetą: https://www.nksc.lt/pranesti.html (žiūrėta 2022-06-08).

[86] Audito kriterijus suderintas 2022-04-15 susitikime su audituojamais subjektais.

[87] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtintas Nacionalinis kibernetinių incidentų valdymo planas, 44 p.

[88] Kibernetinio saugumo įstatymas, 13 str.; Nacionalinis kibernetinių incidentų valdymo planas, 46 p.

[89] Nacionalinis kibernetinių incidentų valdymo planas, 22 p.

nusikalstamos veikos požymių, nes tokios informacijos nerenka. LP nevertina, ar kibernetinis incidentas galėjo paveikti subjektų ryšius, informacines sistemas, ar jis galėjo būti susijęs su asmens duomenų saugumo pažeidimais, todėl pranešimų dėl tokių atvejų NKSC ir VDAI neperduoda;

- 2019–2020 m. laikotarpiu NKSC turėjo 4 atvejus, kai gavę informaciją apie kibernetinį incidentą ir nustatę, kad jis gali turėti nusikalstamos veikos požymių, informaciją perdavė LP (360 kartų siūlė kreiptis į LP patiems subjektams), ir 2 atvejus, kai gavę informaciją apie incidentą ir nustatę, kad jis gali būti susijęs su asmens duomenų saugumo pažeidimais, informaciją perdavė VDAI (24 kartus siūlė kreiptis į inspekciją patiems subjektams). 2020 m. šalyje buvo registruota 4 330 kibernetinių incidentų [90], iš jų 1 966 buvo kenkimo programinė įranga, 61 – sėkmingų įsilaužimų atvejai, 75 – paslaugų trikdymai (angl. *DDoS*). Iš viso 2 102 (arba 48,5 proc.) incidentai, kurie galimai turi nusikalstamos veikos požymių, todėl apie juos LP turėjo būti informuota, tačiau 2020 m. buvo tik 2 atvejai, kai NKSC gavę informaciją apie kibernetinį incidentą bei nustatę, kad jis gali turėti nusikalstamos veikos požymių, informaciją perdavė LP;
- Audituojamu laikotarpiu[91] VDAI gavo 111 pranešimų apie asmens duomenų saugumo pažeidimus, kuriuos pateikė kibernetinio saugumo subjektai ir kurie galimai turėjo nusikalstamos veikos požymių bei galėjo paveikti subjektų ryšių ir informacinių sistemų saugumą. Iš jų 21 galimai turėjo nusikalstamos veikos požymių (dėl 10 buvo pranešta LP), 11 galėjo paveikti kibernetinio saugumo subjektų ryšių ir informacines sistemas (dėl 9 buvo pranešta NKSC).

KIVT institucijos nesudaro prielaidų greitai atpažinti skirtingo pobūdžio kibernetinius incidentus ir perduoti kompetentingoms institucijoms informaciją, kad pastarosios galėtų laiku atlikti nusikalstomų veikų ar pažeidimų užkardymą, dėl to gali nukentėti kibernetinio saugumo subjektai ir visuomenė.

34. Problema, kad teisėsaugos institucijos negauna visos informacijos, identifikuota 2016 m. ES Tarybos vertinimo ataskaitoje apie Lietuvą[92], kurioje atkreipiamas dėmesys, kad Lietuvoje užregistruojama didelė dalis kibernetinių incidentų, tačiau nusikalstamų veikų užregistruojama kur kas mažiau ir nėra duomenų, ar apie visus NKSC užfiksuotus kibernetinius incidentus, turinčius nusikalstamos veikos požymių, yra informuojama LP ir prokuratūra, kaip LP apdoroja gautą informaciją.

35. Viena NKSC funkcijų – valdyti KSIT[93], valstybės informacinę sistemą, kurios paskirtis – IT priemonėmis tvarkyti duomenis, surinktus techninėmis kibernetinio saugumo priemonėmis, siekiant užkardyti ir valdyti kibernetinius incidentus, keistis informacija apie galimus ir įvykusius incidentus, taip pat kita su kibernetinio saugumo užtikrinimu susijusia informacija[94]. Kibernetinio saugumo subjektai ir KIVT institucijos informaciją apie patirtą incidentą (nurodytą Nacionaliniame kibernetinių incidentų valdymo plane) turi perduoti per KSIT, o jeigu tokios galimybės nėra, kitomis saugiomis informacijos

[90] Prieiga per internetą: https://www.nksc.lt/aktualu.html (Nacionalinio kibernetinio saugumo būklės 2020 m. ataskaita, žiūrėta 2022-08-08).

[91] 2019–2021 m.

[92] Europos Sąjungos Taryba, Septintasis tarpusavio vertinimo etapas „Europos kibernetinių nusikaltimų prevencijos ir kovos su tokiais nusikaltimais politikos praktinis įgyvendinimas ir veikimas“. Įvertinimo ataskaita apie Lietuvą, 2016-04-21.

[93] Krašto apsaugos ministro 2013-12-31 įsakymu Nr. V-1200 patvirtinti Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos nuostatai, 10.7 pp.

[94] Kibernetinio saugumo įstatymas, 13 str. 1 d.

perdavimo priemonėmis[95]. NKSC paaiškino, kad informacija apie kibernetinius incidentus iš subjektų ir KIVT institucijų teikiama kitomis priemonėmis: interneto svetainėje[96] ir elektroniniu paštu[97], o apibendrinama KSIT kibernetinių incidentų valdymo posistemėje.

36. Įvertinus NKSC pateiktą informaciją dėl KSIT naudotojų nustatėme, kad 2021 m. didžioji dalis (92 proc.) valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros valdytojų buvo prisijungę prie KSIT, tačiau NKSC nepateikė informacijos apie faktinį naudojimąsi tinklu. Atlikus kibernetinio saugumo subjektų apklausą nustatėme, kad didžioji dalis (59 proc., arba 125 iš 212) jų per pastaruosius 3 mėn. nesinaudojo KSIT. Suinteresuotų institucijų nuomone, KSIT šiuo metu neveikia efektyviai ir galėtų būti plačiau pritaikytas naudojimui (pavyzdžiai).

Suinteresuotų institucijų nuomonės dėl Kibernetinio saugumo informacinio tinklo

IRD: tinklas veikia, tačiau praktinės naudos nėra. KSIT neveikė kelis metus ir tik neseniai buvo atnaujintas. Įprastai informacija apie kibernetinius incidentus keičiasi el. paštu.

RRT: yra prisijungę prie tinklo, tačiau informacijos per šį tinklą neteikia. Tinklas gali būti nepatogus, kadangi reikia žinių kaip naudotis tinklu. RRT dažniau naudojasi el. paštu ar kitomis sistemomis.

VDAI: KSIT nesinaudoja, formaliai KSIT yra, bet praktiškai juo naudojamasi mažai.

KAM: norėtųsi platesnio šio tinklo pritaikymo naudojimui, nes šiuo metu jis yra neefektyvus. Reiktų apibrėžti, kas galėtų naudotis KSIT ir kurti pasitikėjimą tarp narių neįsileidžiant subjektų prižiūrėtojų.

37. Tobulėjančios technologijos sudaro geresnes sąlygas vykdyti incidentus anonimiškai ir tokia veikla gali būti sunkiau atsekama, todėl sklandus komunikavimas apie kibernetinius incidentus laiku leistų analizuoti aktualias jų tendencijas, kurios atitinkamoms institucijoms būtų viena sprendimo kaip juos suvaldyti priėmimo priemonių.

2.2. Kibernetinio saugumo pratybos, mokymai ir konsultacijos vykdomos, tačiau yra nepakankamos siekiant stiprinti subjektų gebėjimus suvaldyti kibernetinius incidentus

38. Sparčiai didėjant kibernetinių atakų skaičiui ir augant jų sudėtingumo lygiui ypač svarbu didinti kibernetinio saugumo subjektų kompetencijas reaguoti į skirtingus incidentus, parengties gebėjimus ir informuotumą kibernetinio saugumo klausimais[98]. Kibernetinio saugumo pratybos ir mokymai organizacijoms suteikia vertingų įžvalgų apie jų pasirengimą reaguoti į realius kibernetinius išpuolius, saugumo politikos veiksmingumą, padeda nustatyti saugumo rizikas ir neatitikties problemas, į kurias reikia nedelsiant reaguoti[99], teorinės ir praktinės žinios apie kibernetines atakas, ypač paremtas socialine inžinerija, gali padėti apsisaugoti silpniausią kibernetinio saugumo grandį – organizacijos darbuotojus.

[95] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtintas Nacionalinis kibernetinių incidentų valdymo planas, 46 p.

[96] Prieiga per internetą: https://www.nksc.lt/ (Pranešti apie incidentą, žiūrėta 2022-06-08).

[97] cert@cert.lt.

[98] Prieiga per internetą: https://www.enisa.europa.eu/publications/enisa-strategy-leaflet-translations/enisa-strategy-leaflet-lt.pdf (žiūrėta 2022-07-25).

[99] Prieiga per internetą: https://www.securityforum.org/in-the-news/10-benefits-of-running-cybersecurity-exercises/ (žiūrėta 2022-07-25).

39. KAM ir NKSC yra atsakingi už kibernetinio saugumo pratybų rengimą, kibernetinio saugumo mokymų organizavimą, konsultacijas ir rekomendacijas, susijusias su šio saugumo užtikrinimu[100].

40. Laikėmės nuostatos, kad KAM ir NKSC vykdoma veikla prisideda prie tinkamo kibernetinio saugumo subjektų gebėjimų suvaldyti kibernetinius incidentus tobulinimo, jeigu:

- 2019–2021 m. nemažiau 95 proc. apklaustų kibernetinio saugumo subjektų nors vieną kartą dalyvavo pratybose[101]; 2019–2021 m. NKSC visa apimtimi įgyvendino suplanuotas pratybas[102]; 90 proc. apklaustų subjektų nurodė, kad NKSC organizuojamos pratybos yra pakankamos[103];
- 2019–2021 m. nemažiau 95 proc. apklaustų kibernetinio saugumo subjektų nors vieną kartą dalyvavo mokymuose[104]; 2019–2021 m. NKSC visa apimtimi įgyvendino suplanuotus mokymus[105]; 90 proc. apklaustų subjektų nurodė, kad NKSC organizuojami mokymai yra pakankami[106];
- 90 proc. apklaustų kibernetinio saugumo subjektų nurodė, kad KAM ir NKSC teikiamos konsultacijos pakankamos[107]; 90 proc. apklaustų kibernetinio saugumo subjektų nurodė, kad KAM ir NKSC skelbiama informacija apie šį saugumą pakankama[108];
- 100 proc. apklaustų kibernetinio saugumo subjektų turi patvirtintus kibernetinių incidentų valdymo planus[109]; patvirtintas tipinis kibernetinių incidentų valdymo planas (geroji praktika: KAM tvirtiną tipinį kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planą)[110].

41. Siekiant formuoti kibernetinio saugumo subjektų kibernetinio saugumo įgūdžius, patikrinti kibernetinių incidentų valdymo procedūras, gerinti bendradarbiavimą tarp KIVT institucijų ir subjektų rengiamos nacionalinės kibernetinio saugumo pratybos[111]. Įvertinus strateginės priemonės įgyvendinimo būklę[112] nustatėme, kad 2019–2021 m. NKSC surengė pratybas kaip buvo suplanuota strateginiuose dokumentuose[113], tačiau strateginis rodiklis (Nacionalinėse kibernetinio saugumo pratybose dalyvaujančių ypatingos svarbos informacinės infrastruktūros valdytojų ir valstybės informacinių išteklių valdytojų ir (arba)

[100] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtinta Nacionalinė kibernetinio saugumo strategija, 12 p., krašto apsaugos ministro 2013-12-31 įsakymu Nr. V-1200 patvirtinti Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos nuostatai, 15.1, 15.2, 16.4, 16.5 pp.

[101] Nacionalinė kibernetinio saugumo strategija, 12 p., 14.3 pp.

[102] Ten pat, Vyriausybės 2019-07-03 nutarimu Nr. 709 patvirtintas Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas, 2 priedas, P-1-3-1, P-1-3-2 vertinimo kriterijai.

[103] Audito kriterijus suderintas 2022-04-15 susitikime su audituojamais subjektais.

[104] Nacionalinė kibernetinio saugumo strategija, 23, 25 p.

[105] Ten pat, Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas, 2 priedas, P-3-2-1 vertinimo kriterijus.

[106] Audito kriterijus suderintas 2022-04-15 susitikime su audituojamais subjektais.

[107] Nacionalinė kibernetinio saugumo strategija, 12 p.

[108] Audito kriterijus suderintas 2022-04-15 susitikime su audituojamais subjektais.

[109] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtintas Nacionalinis kibernetinių incidentų valdymo planas, 22 p.

[110] Kibernetinio saugumo įstatymas, 6 str. 6 p.

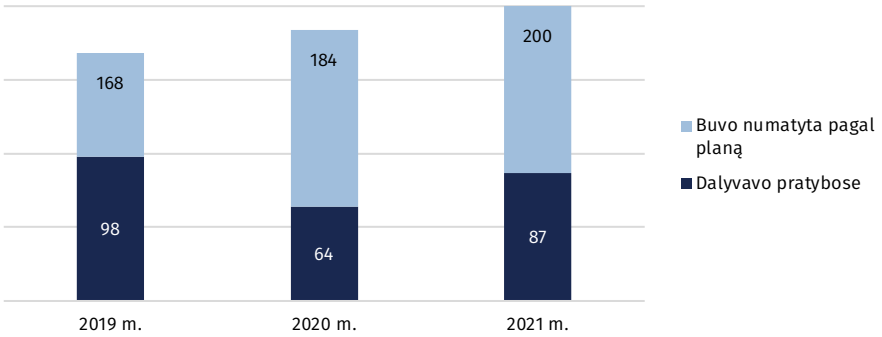
[111] Nacionalinė kibernetinio saugumo strategija, 14.3 pp.

[112] Nacionalinė kibernetinio saugumo strategija, Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas, 1 priedas, 1-3-1 priemonė ir 2 priedas, P-1-3-1 vertinimo kriterijus.

[113] Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas, 1 priedas, 1-3-1 priemonė.

tvarkytojų skaičius)[114] per tris metus (2019–2021 m.) nė karto nebuvo pasiektas (2 pav.), 2020 m. ypač mažą ypatingos svarbos informacinės infrastruktūros valdytojų ir valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų įsitraukimą (vietoj planuotų 184[115] dalyvavo 64[116] subjektai) lėmė veiklų ribojimai ir pokyčiai dėl COVID-19 pandemijos.

2 pav. 2019–2021 m. nacionalinėse kibernetinio saugumo pratybose dalyvavusių ypatingos svarbos informacinės infrastruktūros valdytojų ir valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų skaičius (vnt.)



Šaltinis – Valstybės kontrolė pagal NKSC duomenis[117]

42. 2019–2021 m. 35 proc. (74 iš 212) apklaustų subjektų nė karto nedalyvavo nacionalinėse kibernetinio saugumo pratybose. Kasmet mažėjo ministerijų dalyvavimas pratybose: 2019 m. – 7 iš 14 ministerijų (arba 50 proc.), 2020 m. – 6 iš 14 (arba 43 proc.), o 2021 m. tik 4 iš 14 (arba 29 proc.)[118].

43. Anot NKSC, ne visi kibernetinio saugumo subjektai dalyvauja nacionalinėse kibernetinio saugumo pratybose dėl nepakankamo organizacijų vadovybės dėmesio šio saugumo klausimams, žmogiškųjų išteklių trūkumo, dėl nepakankamo vadovaujančių institucijų dalyvavimo pratybose[119] ir dėl to, kad teisės aktai nenustato prievolės subjektams dalyvauti tokiose pratybose. Apklausti subjektai dažniausiai nurodė, kad nedalyvavo pratybose dėl personalo trūkumo (49 proc., arba 24 iš 49 į klausimą atsakiusiųjų) ar negavo kvietimo jose dalyvauti (18 proc., arba 9 iš 49). Dalyvavimas pratybose padėtų ugdyti subjektų įgūdžius laiku reaguoti į realius kibernetinius išpuolius, suteiktų jiems įžvalgų apie galimas valdomų ryšių ir informacinių sistemų saugumo spragas.

44. NKSC po pratybų vykdytose apklausose 90–96 proc. vietinių instruktorių pritarė teiginiui, kad 2019–2021 m. pratybos jų organizacijai buvo naudingos[120]. Atlikta kibernetinio saugumo subjektų apklausa parodė, kad 73 proc. (arba 101 iš 138) subjektų NKSC organizuojamas kibernetinio augumo pratybas vertina kaip pakankamas (3 pav.). Manantys, kad pratybos iš dalies pakankamos (23 proc., arba 32 iš 138) ar nepakankamos (4 proc., arba 5 iš 138), pažymi, kad pratybos turėtų atitikti jų organizacijų vykdomas

[114] Vyriausybės 2019-07-03 nutarimu Nr. 709 patvirtintas Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas, 2 priedas, P-1-3-1 vertinimo kriterijus.

[115] Ten pat: 2020 m. siektina reikšmė.

[116] Prieiga per internetą: https://www.nksc.lt/doc/KS2020_pratybu_ataskaita.pdf (žiūrėta 2022-06-29).

[117] Prieiga per internetą: https://www.nksc.lt/aktualu.html (2019, 2020 ir 2021 m. pratybų „Kibernetinis skydas“ ataskaitos, žiūrėta 2022-06-29).

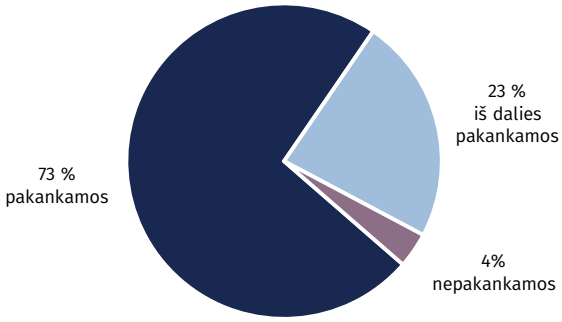
[118] Ten pat.

[119] Jei pratybose nedalyvauja vadovaujanti ministerija, todėl pavaldžios įstaigos irgi renkasi nedalyvauti.

[120] Prieiga per internetą: https://www.nksc.lt/aktualu.html (2019, 2020 ir 2021 m. pratybų „Kibernetinis skydas“ ataskaitos, žiūrėta 2022-06-29).

funkcijas ir realias grėsmes, apimti visus įstaigų darbuotojus, turėtų būti labiau orientuotos į specifinių IT žinių neturinčius darbuotojus. Subjektai pasigedo didelio ar vidutinio poveikio incidento suvaldymo scenarijaus, kai būtų derinami visų pratybų dalyvių veiksmai, t. y. organizacijos, kuri patiria ataką, IT specialistų, NKSC, padedančių ištirti ir valdyti incidentą, ekspertų, LKPB, padedančių išsaugoti įrodymus ir juos ištirti, ekspertų ir elektroninių ryšių paslaugų teikėjų.

3 pav. Kibernetinio saugumo subjektų nuomonė apie nacionalines kibernetinio saugumo pratybas (proc.)



Šaltinis – Valstybės kontrolė pagal kibernetinių subjektų apklausos duomenis

45. Atlikta kibernetinio saugumo subjektų apklausa rodo, kad prieš kibernetinio saugumo pratybas 41 proc. (arba 56 iš 138) subjektų savo saugumo žinias ir įgūdžius įvertino kaip geras arba labai geras, o po pratybų – 59 proc. (arba 82 iš 138). Dauguma (78–89 proc. iš 138 atsakiusių į teiginius) dalyvavusiųjų sutinka, kad pratybos gerai organizuotos, aktualios ir stiprinančios jų gebėjimus.

46. Nesiimant teisinių veiksmų, kuriais būtų užtikrinamas kibernetinio saugumo subjektų įsitraukimas dalyvauti šio saugumo pratybose, nepakankamai išnaudojamos galimybės stiprinti šiuos gebėjimus NKSC organizuojamose kibernetinio saugumo pratybose.

47. NKSC nurodė, kad 2019–2021 m. centras organizavo kibernetinio saugumo mokymus, kuriuose 2019 m. buvo daugiau kaip 470 dalyvių[121], 2020 m. – 778 dalyviai (iš jų 398 viešojo sektoriaus darbuotojai), 2021 m. – 3 159 dalyviai (iš jų 2 205 viešojo sektoriaus darbuotojai). 2021 m. padidėjo mokymuose dalyvavusių kibernetinio saugumo subjektų skaičius, tačiau atlikta apklausa parodė, kad organizuojami kibernetinio saugumo mokymai nesudaro sąlygų stiprinti gebėjimus visiems kibernetinio saugumo subjektams, nes 2019–2021 m.:

    - didžioji dalis (52 proc., arba 110 iš 212) apklaustų subjektų nė karto nedalyvavo mokymuose, nes nebuvo pakviesti arba nedalyvavo dėl riboto dalyvių skaičiaus;
    - dauguma (72 proc., arba 73 iš 102) apklaustų ir mokymuose dalyvavusių subjektų juos įvertino gerai.

48. Jei kibernetinio saugumo subjektai reguliariai dalyvautų mokymuose, jų mokymų poreikis būtų vertinimas kaip pakankamas, būtų užtikrintas darbuotojų kibernetinio saugumo kompetencijų stiprinimas, didėtų atsakomybė ir atsparumas kibernetinėms grėsmėms.

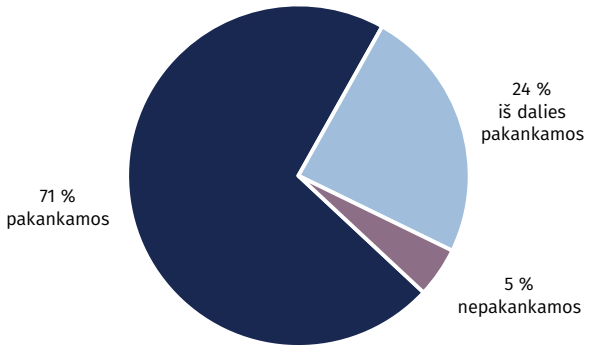
49. Kibernetinio subjektų apklausa parodė, kad:

    - 71 proc. (150 iš 212) apklaustų kibernetinio saugumo subjektų mano, kad KAM ir NKSC teikiamos konsultacijos kibernetinio saugumo tematika yra pakankamos, 24 proc. (52 iš 212) – iš dalies pakankamos, 5 proc. (10 iš 212) mano, kad konsultacijų nepakanka

[121] NKSC nepateikė tikslaus 2019 m. mokytų kibernetinio saugumo subjektų darbuotojų skaičiaus.

(4 pav.), 29 proc. (62 iš 212) apklaustųjų nurodė, kad labiausiai trūksta konsultacijų susijusių su teisinio reglamentavimo išaiškinimu, praktiniu kibernetinio saugumo politikos įgyvendinimu, pasigendama dažnesnių, detalesnių, struktūriškų ir įvairesnio spektro pranešimų kibernetinio saugumo tematika, grįžtamojo ryšio po kibernetinių incidentų, aiškesnių atsakymų konsultuojant kibernetinio saugumo subjektus.

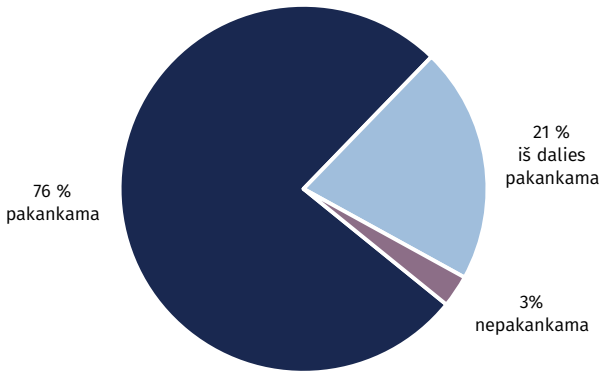
4 pav. Kibernetinio saugumo subjektų nuomonė apie Krašto apsaugos ministerijos ir Nacionalinio kibernetinio saugumo centro teikiamas konsultacijas kibernetinio saugumo tematika (proc.)



Šaltinis – Valstybės kontrolė pagal kibernetinių subjektų apklausos duomenis

- 76 proc. (162 iš 212) apklaustų kibernetinio saugumo subjektų nurodė, kad KAM ir NKSC viešai skelbiama informacija yra pakankama, 21 proc. (44 iš 212) – iš dalies pakankama, 3 proc. (6 iš 212) – nepakankama (5 pav.). Subjektai nurodo, kad trūksta konsultacijų ir (ar) metodikų, susijusių su teisinio reglamentavimo išaiškinimu, praktiniu kibernetinio saugumo politikos įgyvendinimu, efektyvesnio komunikavimo, grįžtamojo ryšio po šių incidentų išsprendimo, pranešimų kibernetinio saugumo tematika.

5 pav. Kibernetinio saugumo subjektų nuomonė apie Krašto apsaugos ministerijos ir Nacionalinio kibernetinio saugumo centro viešai skelbiamą informaciją kibernetinio saugumo tematika (proc.)



Šaltinis – Valstybės kontrolė pagal kibernetinių subjektų apklausos duomenis

50. Kibernetinio saugumo pratybos, mokymai ir konsultacijos kibernetinio saugumo klausimais suteikia kibernetinio saugumo subjektams svarbių įžvalgų apie jų pasirengimą reaguoti į incidentus, gebėjimą užkirsti jiems kelią, būtinybę patikrinti atsparumo ir gynybos strategiją, incidentų valdymo planų efektyvumą, atitiktį teisės aktų reikalavimams, ir didina darbuotojų atsparumą socialine inžinerija paremtoms kibernetinėms atakoms. Nevykdant pakankamo švietimo kibernetinio saugumo klausimais, nebus užtikrintas sistemingas šio saugumo subjektų gebėjimų suvaldyti kibernetinius incidentus tobulinimas, aukšta kibernetinio saugumo kultūra.

51. Kibernetinių incidentų valdymo planas svarbus, nes jame turi būti nustatytos tipinės procedūros, siekiant tinkamai valdyti identifikuotus kibernetinius incidentus. Teisės aktuose numatyta[122], kad subjektai kibernetinių incidentų tyrimą atlieka vadovaudamiesi savo patvirtintais kibernetinio saugumo teisės aktais tiek, kiek to nereglamentuoja Nacionalinis kibernetinių incidentų valdymo planas, ir imasi visų įmanomų priemonių, būtinų kibernetiniam incidentui suvaldyti ir įprastai ryšių ir IS veiklai atkurti, tačiau subjektų apklausa parodė, kad 26 proc. (55 iš 212) apklaustųjų nėra parengę ir patvirtinę šių incidentų valdymo plano arba tvarkos.

52. KAM įstatymu suteikti įgaliojimai tvirtinti tipinį kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planą[123], kuriame turi būti nustatytos kibernetinio saugumo subjektų taikomos procedūros, leidžiančios tinkamai valdyti šiuos incidentus. Planas patvirtintas[124], bet jis nuo 2019-01-01 negalioja. Didžioji dalis (90 proc., arba 190 iš 212) apklaustų subjektų mato poreikį parengti tipinį kibernetinių incidentų valdymo planą.

53. Siekiant sudaryti sąlygas, kad visi kibernetinio saugumo subjektai žinotų veiksmus, kurių reikia imtis įvykus kibernetiniam incidentui, veiksmingiau juos valdyti bei užkirsti kelią galimoms grėsmėms, reikia parengti ir patvirtinti detalų tipinį kibernetinių incidentų valdymo planą ir įpareigoti subjektus, pagal šio standartinio plano pavyzdį, parengti ar atnaujinti savo vidinius kibernetinių incidentų valdymo planus ar tvarkas.

3. NEUŽTIKRINAMAS NUOSEKLUS KIBERNETINIO SAUGUMO PLANAVIMO ĮGYVENDINIMAS

54. Nacionalinė kibernetinio saugumo strategija[125] yra pagrindinis planavimo dokumentas, kuriame nustatytos 2018–2023 m. viešojo ir privataus sektorių, Lietuvos mokslo ir studijų institucijų kibernetinio saugumo stiprinimo kryptys, tikslai ir uždaviniai. Strategijos tikslų ir uždavinių įgyvendinimo 2019–2021 m. priemonės ir asignavimai joms įgyvendinti numatyti Tarpinstituciniame veiklos plane[126].

55. Dėl valstybės strateginio valdymo pertvarkos[127], nuo 2021 m. įtvirtinti nauji strateginio planavimo dokumentų tipai (nebeliko strategijų ir tarpinstitucinių veiklos planų)[128]. KAM pavesta iki 2022 IV ketv. parengti naują strateginio planavimo dokumentą – Nacionalinę kibernetinio saugumo plėtros programą[129], kuri apibrėžtų naujas pažangos (kibernetinio saugumo stiprinimo) priemones ir turėtų pakeisti Strategiją.

---

[122] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtintas Nacionalinis kibernetinių incidentų valdymo planas, 22 p.

[123] Kibernetinio saugumo įstatymas, 6 str. 6 p.

[124] Vyriausybės 2016-07-20 nutarimu Nr. 746 patvirtintas Tipinis kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planas (galiojo iki 2018-12-31).

[125] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtinta Nacionalinė kibernetinio saugumo strategija.

[126] Vyriausybės 2019-07-03 nutarimu Nr. 709 patvirtintas Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas.

[127] Nuo 2021-01-01 įsigaliojo Strateginio valdymo įstatymas.

[128] Strateginio valdymo įstatymas, 9 str.

[129] Kibernetinio saugumo įstatymas, 6 str. 1^1 p., Vyriausybės 2021-03-10 m. nutarimu Nr. 155 patvirtintas Aštuonioliktosios Lietuvos Respublikos Vyriausybės programos nuostatų įgyvendinimo planas, 11.4.4 priemonė.

56. Laikėmės nuostatos, kad nuoseklus kibernetinio saugumo planavimo įgyvendinimas yra užtikrinamas, jeigu:

- kiekvienais metais visi numatyti Strategijos įgyvendinimo vertinimo kriterijai visiškai pasiekti[130];
- visi numatyti tarpiniai Strategijos įgyvendinimo vertinimo kriterijai visiškai pasiekti[131];
- kiekvienais metais visos suplanuotos priemonės, kurios sudaro sąlygas pasiekti Strategijos tikslus ir uždavinius, visiškai įgyvendintos[132];
- kiekvienais metais peržiūrimi plano priemonių įgyvendino rezultatai[133];
- kai buvo vėlavimo ar neįvykdymo požymių, visais atvejais Strategijos priemonių vykdytojai ėmėsi priemonių šiuos atvejus valdyti ar koreguoti[134];
- kai buvo vėlavimo ar neįvykdymo požymių ir visais atvejais Strategijos priemonių vykdytojai nesiėmė priemonių šiuos atvejus valdyti ar koreguoti, strategijos koordinatorius ėmėsi veiksmų spręsti ar koordinuoti neįgyvendinimo priežastis[135].

57. Strategijos tikslams ir uždaviniams įgyvendinti Tarpinstituciniame veiklos plane[136] numatytos 28 priemonės ir kiekvienų metų asignavimai joms įgyvendinti[137], priemonių įgyvendinimo terminai nėra nurodyti. Atlikus 2019 ir 2020 m. Nacionalinės kibernetinio saugumo strategijos įgyvendinimo ataskaitų [138] ir Strategijos vykdytojų [139] pateiktų duomenų apie priemonių įgyvendinimą ir asignavimų panaudojimą 2021 m. analizę nustatėme, kad 2019–2021 m. iš 28 priemonių: 17 įgyvendinta[140], 4[141] neįgyvendintos (2 lentelė), 7 buvo vykdytos ir įgyvendinamos, tačiau dėl COVID-19 pandemijos, neįvykusių viešųjų pirkimų procedūrų ar KAM baigtos priemonių įgyvendinimo stebėsenos[142], jos įgyvendintos ne visa apimtimi arba nežinoma jų įgyvendinimo būklė. Pvz., 3.1.2 priemonė[143] vykdyta 2019–2021 m., bet 2020 m. dėl COVID-19 pandemijos metu atsiradusių prekių stygiaus ir vėluojančio prekių pristatymo panaudota 57 proc. (45,9 tūkst. iš 80 tūkst. Eur) numatytų asignavimų, 2021 m. – 18 proc. (33,2 tūkst. iš 180 tūkst. Eur), vėluoja 2019–2021 m. vykdytos 3.2.2 priemonės[144] įgyvendinimas, dėl COVID-19 pandemijos pirmieji kompleksiniai kibernetinio saugumo mokymai vyko 2021 m. sausio–

[130] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtinta Nacionalinė kibernetinio saugumo strategija, 43, 46 p., Vyriausybės 2019-07-03 nutarimu Nr. 709 patvirtintas Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas, 8 p. ir 2 priedas.

[131] Nacionalinė kibernetinio saugumo strategija, 46 p., priedas.

[132] Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas, 5, 6, 7 ir 8 p.

[133] Strateginio valdymo įstatymas, 3 str. 20 d., 18 str. 5 d., Nacionalinė kibernetinio saugumo strategija, 48 p.

[134] Cobit®5: Enabling Processes, EDM02 „Užtikrinti naudos sukūrimą“, APO02 „Valdyti strategiją“, MEA01 „Stebėti, vertinti ir įvertinti veiklos efektyvumą ir atitiktį“, procesų aprašymai, 35-37; 57-62; 203-206 psl.

[135] Ten pat.

[136] Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas.

[137] Ten pat, 1 ir 2 priedai.

[138] Prieiga per internetą: https://www.nksc.lt/aktualu.html (Nacionalinės kibernetinio saugumo strategijos įgyvendinimo ataskaitos, žiūrėta 2022-06-29).

[139] KAM, VRM, TM, URM, ŠMSM, RRT.

[140] Iš 17 priemonių 2019 m. įgyvendintos 3; 2020 m. – 2, 2021 m. – 12.

[141] 2 (iš 4) priemonė nepradėta vykdyti, nors asignavimai buvo numatyti, 2 (iš 4) – vykdytos ir neįgyvendintos.

[142] Nuo 2021-01-01 įsigaliojus Strateginio valdymo įstatymui, Krašto apsaugos ministerija nevykdė priemonių įgyvendinimo stebėsenos.

[143] 3.1.2 priemonė: sukurti saugų kriptografiniais metodais pagrįstą dalijimosi informacija būdą.

[144] 3.2.2 priemonė: įgyvendinti projektą „Kompleksiniai kibernetinės saugos mokymai valstybės ir savivaldybių institucijų ir įstaigų dirbantiesiems“.

gegužės mėn. pagal tris parengtas programas, 2022 m. numatyta parengti ir pasiūlyti dar dvi mokymų programas[145].

2 lentelė. Neįgyvendintos Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano priemonės

Priemonės pavadinimas, numatyti asignavimai ir atsakingas Strategijos vykdytojas[146]	Priemonės būklė ir Strategijos vykdytojų nuodytos neįgyvendinimo priežastys
1.1.3 priemonė – atnaujinti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemą (ARSIS); 130 tūkst. Eur; KAM.	Neįgyvendinta, nes 2020 m. atlikus ARSIS turimo programinio kodo keitimo analizę nustatyta, kad pagal turimą programinį kodą nėra galimybės atlikti ARSIS funkcinio praplėtimo arba yra didelė rizika ARSIS funkcionalumus pažeisti ir nebeatkurti.
1.2.1 priemonė – parengti kaštų ir naudos kibernetiniam saugumui užtikrinti analizės ir kontrolės modelį, siekiant sudaryti galimybes kibernetinio saugumo subjektams planuoti kibernetiniam saugumui užtikrinti skirtas lėšas; 100 tūkst. Eur; KAM.	Nepradėta vykdyti dėl COVID-19 pandemijos.
3.1.3 priemonė – sukurti nacionalinio kibernetinio saugumo aplinkos rizikų vertinimo ir sprendimų priėmimo metodiką ir jai įgyvendinti reikalingus įrankius; 100 tūkst. Eur; KAM.	Nepradėta vykdyti dėl KAM suplanuotų esminių pokyčių kibernetinio saugumo reikalavimų taikymo ir jų įgyvendinimo stebėsenos sistemoje.
3.2.1 priemonė – sukurti Valstybės tarnautojų registro ir valstybės tarnybos valdymo informacinės sistemos modulį, skirtą valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartis, mokymams, tarp jų – kibernetinio saugumo; 411,6 tūkst. Eur; VRM.	Neįgyvendinta, priemonė yra sudedamoji projekto „Inovatyvių informacinių technologijų, skirtų efektyviam viešojo valdymo sektoriaus žmogiškųjų išteklių valdymui, sukūrimas ir įdiegimas“[147] dalis. 2020 m. vyko organizaciniai pokyčiai[148], susiję su projekto vykdytojų pasikeitimu, 2021 m. priimtas sprendimas priemonę įgyvendinti kartu su kitomis priemonėmis[149].

Šaltinis – Valstybės kontrolė pagal Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano 2019–2020 m. ataskaitas ir KAM, VRM, TM, URM, ŠMSM, RRT pateiktus duomenis

58. 2019–2021 m. priemonėms įgyvendinti iš viso buvo numatyta 9 705,1 tūkst. Eur[150]:

- 2019 m. 1 583,2 tūkst. Eur, iš jų dėl sutaupymo panaudota 97,1 proc. (arba 1537,9 tūkst. Eur);
- 2020 m. iš 3 389,8 tūkst. Eur priemonėms skirtų asignavimų dėl ne visa apimtimi vykdytų priemonių panaudoti 66 proc. (arba 2236,3 tūkst. Eur);
- 2021 m. suplanuota 4 732,1 tūkst. Eur, tačiau asignavimų panaudojimo procentas nėra žinomas, nes KAM nepateikė informacijos apie 2021 m. panaudotus asignavimus.

[145] Prieiga per internetą: https://www.nksc.lt/aktualu.html (Nacionalinės kibernetinio saugumo strategijos įgyvendinimo ataskaitos, žiūrėta 2022-06-29), NKSC 2021-ųjų metų veiklos ataskaita.

[146] Vyriausybės 2019-07-03 nutarimu Nr. 709 patvirtintas Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas, 1 priedas.

[147] Projekto Nr. 10.1.5-ESFA-V923-01-0006 „Inovatyvių informacinių technologijų, skirtų efektyviam viešojo valdymo sektoriaus žmogiškųjų išteklių valdymui, sukūrimas ir įdiegimas“ sutartis Nr. 10.1.5-ESFA-V923-01-0006/27F11-88 pasirašyta 2018-10-20.

[148] 2020-03-10 projekto vykdymas iš Valstybės tarnybos departamento prie VRM buvo perduotas IRD.

[149] 2022-06-03 Centrinėje viešųjų pirkimų informacinė sistemoje paskelbtas pirkimas Bendros informacinės sistemos valstybės įstaigų personalui administruoti bei inovatyvių informacinių technologijų, skirtų efektyviam viešojo valdymo sektoriaus žmogiškųjų išteklių valdymui sukūrimo, tobulinimo ir įdiegimo paslaugų įsigijimui iš kelių finansavimo šaltinių.

[150] Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas, 1 priedas.

59. Pokytis strateginėse kibernetinio saugumo stiprinimo kryptyse vertinamas pagal Strategijos įgyvendinimo vertinimo kriterijus ir siekiamas jų reikšmes [151]. Tarpinstituciniame veiklos plane[152] iš viso numatyti 38 vertinimo kriterijai (2[153] Strategijos pagrindinio tikslo [154] pasiekimo arba efekto rodikliai [155], 11 [156] – Strategijos tikslų [157] pasiekimo arba rezultato rodikliai[158], 25[159] – Strategijos uždavinių[160] įgyvendinimo arba produkto rodikliai[161]) ir jų siektinos reikšmės 2019–2021 m.

60. Atlikus 2019–2021 m. Strategijos įgyvendinimo pasiektų rezultatų [162] palyginimą su numatytais strateginiais rodikliais [163] nustatėme, kad nors audituojamu laikotarpiu Strategijos efekto rodikliai (Lietuvos vieta pasauliniame kibernetinio saugumo indekse ir kibernetinių incidentų grėsmės lygis) yra pasiekti, tačiau kiti Strategijos įgyvendinimo vertinimo kriterijai ne visi ir ne kiekvienais metais yra pasiekti (6 pav.): 2019 m. nepasiekti 5 strateginiai rodikliai ir 1 reikšmė nežinoma, 2020 m. – 13, 2021 m. – 9 ir dar 5 rodiklių reikšmė nežinoma dėl KAM baigtos Strategijos įgyvendinimo stebėsenos[164].

[151] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtinta Nacionalinė kibernetinio saugumo strategija, 46 p., Vyriausybės 2019-07-03 nutarimu Nr. 709 patvirtintas Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas, 2 priedas.

[152] Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas.

[153] E-1, E-2 pagal Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos plano 2 priedo numeraciją.

[154] Nacionalinė kibernetinio saugumo strategija, 4 p.

[155] Vyriausybės 2022-04-28 nutarimu Nr. 292 patvirtinta Strateginio valdymo metodika, 186.1 pp. (iki 2021-04-21 Vyriausybės 2002-06-06 nutarimu Nr. 827 patvirtinta Strateginio planavimo metodika, 48 p.).

[156] R-1-1, R-1-2, R-1-3, R-1-4, R-2-1, R-2-2, R-3-1, R-3-2, R-4-1, R-5-1, R-5-2 pagal Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos plano 2 priedo numeraciją.

[157] Nacionalinė kibernetinio saugumo strategija, 5, 15, 23, 33, 39 p.

[158] Strateginio valdymo metodika, 186.2 pp. (iki 2021-04-21 Strateginio planavimo metodika, 48 p.).

[159] Vertinimo kriterijų kodas su „P“ raide (P-1-1-1, P-1-1-2 ir kiti) pagal Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos plano 2 priedo numeraciją.

[160] Nacionalinė kibernetinio saugumo strategija, 14, 22, 32, 38, 42 p.

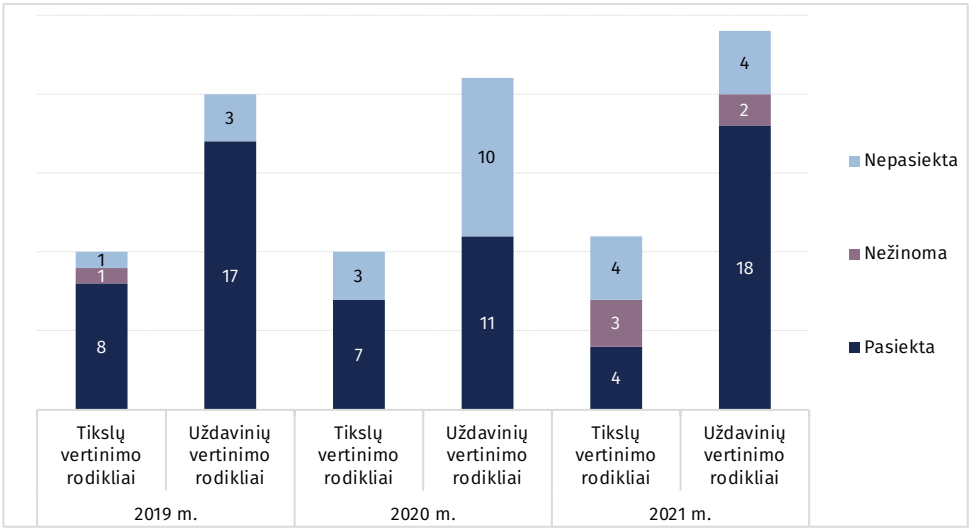
[161] Strateginio valdymo metodika, 186.3 pp. (iki 2021-04-21 Strateginio planavimo metodika, 48 p.).

[162] Prieiga per internetą: https://www.nksc.lt/aktualu.html (2019 ir 2020 m. Nacionalinės kibernetinio saugumo strategijos įgyvendinimo ataskaitos, žiūrėta 2022-06-29), KAM, VRM, TM, ŠMSM, URM, RRT duomenys apie vertinimo kriterijų pasiekimą 2021 m.

[163] Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas, 2 priedas.

[164] Nuo 2021-01-01 įsigaliojus Strateginio valdymo įstatymui, Krašto apsaugos ministerija nevykdė Strategijos įgyvendinimo stebėsenos.

6 pav. 2019–2021 m. Strategijos tikslų ir uždavinių įgyvendinimo būklė pagal vertinimo kriterijus (vnt.)



Šaltinis – Valstybės kontrolė pagal KAM, VRM, TM, URM, ŠMSM, RRT duomenis

61. Atlikę tarpinių[165] Strategijos įgyvendinimo rezultatų analizę nustatėme, kad nepakankama pažanga (vertinant 2021 m. Strategijos įgyvendinimo vertinimo kriterijų reikšmes) stebima įgyvendinant uždavinius, susijusius su atitikties elektroninės informacijos saugos reikalavimas stebėsenos sistemos modernizavimu (žr. 1.2 poskyrį, 15 psl.), kibernetinio saugumo subjektų kibernetinio saugumo kultūros skatinimu (subjektų dalyvavimu pratybose ir mokymuose, žr. 2.2 poskyrį, 23 psl.), viešojo ir privataus sektorių bendradarbiavimo stiprinimu (komunikavimu apie kibernetinius incidentus, žr. 2.1 poskyrį, 21 psl.), kibernetinės gynybos plėtra, inovacijomis kibernetinio saugumo srityje.

62. Geroji IT valdymo praktika rekomenduoja nuolat vertinti veiklos efektyvumą, stebint patvirtintų rodiklių (vertinimo kriterijų) pasiekimą, o esant nuokrypiams, inicijuoti, nustatyti ir stebėti koregavimo veiksmus[166]. KAM koordinuoja ir vykdo Strategijos įgyvendinimo rezultatų stebėseną[167]. Strategijos įgyvendinimo stebėsenos tvarka[168] yra orientuota į nuolatinį atsiskaitymą už pasiektą pažangą, tačiau jos įgyvendinimo rezultatai nebuvo peržiūrimi kasmet. Strategijos pažangos stebėsena buvo vykdoma 2019 ir 2020 m., o 2021 m. Strategijos koordinatorius[169] nerinko ir nesistemino duomenų apie Strategijos ir plano įgyvendinimą. Patys Strategijos vykdytojai stebėjo ne visas priemones ir vertinimo kriterijus, todėl neturi informacijos apie:

- 7[170] iš 28 Tarpinstituciniame veiklos plane numatytų priemonių įgyvendinimo būklę;
- 5[171] iš 36 numatytų Strategijos įgyvendinimo vertinimo kriterijų reikšmę.

[165] 2021 m.

[166] Cobit®5: Enabling Processes, MEA01.05 „Ensure the implementation of corrective actions“ bazinės praktikos aprašymas, 206 psl.

[167] Vyriausybės 2018-08-13 nutarimu Nr. 818 patvirtinta Nacionalinė kibernetinio saugumo strategija, 46 ir 49 p.

[168] Ten pat, 46-50 p.

[169] Krašto apsaugos ministerija.

[170] Vyriausybės 2019-07-03 nutarimu Nr. 709 patvirtintas Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas, 1 priedas 1.1.4, 1.1.5, 1.4.1, 1.4.2, 1.4.3, 2.2.1, 3.1.3 pp.

[171] Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas, 2 priedas, R-2-1, R-2-2, R-3-2, P-3-1-2, P-3-2-1 vertinimo kriterijai.

63. KAM nurodo, kad dėl strateginio valdymo pertvarkos (žr. 55 p.), nuo 2021 m. ministerija nevykdė Strategijos įgyvendinimo stebėsenos ir vertinimo. Auditorių nuomone, kol Nacionalinės kibernetinio saugumo strategija ir Tarpinstitucinis veiklos planas yra galiojantys teisės aktai[172], jų numatyti tikslai ir uždaviniai bei jiems pasiekti numatytos priemonės turėjo būti įgyvendinami, vykdoma jų stebėsena ir atsiskaitymas už rezultatus, o Strategijos įgyvendinimo rezultatai galėjo būti panaudoti rengiant naujus strateginio planavimo dokumentus[173].

64. Nors 2019–2021 m. ne visos suplanuotos priemonės buvo įgyvendinamos numatyta apimtimi, ne visi strateginiai rodikliai pasiekti, tačiau strateginių tikslų ir uždavinių neįvykdymo rizikos nebuvo valdomos: kai buvo vėlavimo ar nevykdymo požymių, Strategijos vykdytojai nepateikė pasiūlymų ar įžvalgų dėl matomų rizikų, probleminių sričių, kurios trukdo įgyvendinti Strategiją, o KAM kaip Strategijos koordinatorius nesiėmė veiksmų spręsti priemonių neįgyvendinimo priežastis.

65. KAM nurodo, kad Strategijos įgyvendinimo problematika yra sisteminio pobūdžio, tad ją buvo bandoma spręsti[174] nacionaliniu lygiu keičiant strateginio planavimo sistemą, taip pat pažymi, kad 2019–2020 m. strategijoje dalyvaujančių institucijų informacijos rinkimas ir apibendrinimas buvo vykdomas rankiniu būdu, nors tam buvo sukurta speciali stebėsenos informacinė sistema. Ministerijos nuomone, rankinis duomenų surinkimas iš Strategijos vykdytojų sukuria didelę administracinę naštą ir nėra efektyvus analizei vykdyti, tad problemų ir rizikų analizei trūko laiko.

66. Svarbu užtikrinti veiksmingą pažangos stebėsenos ir kontrolės sistemą, kuri leistų įvertinti pasiektus rezultatus, įgyvendinant esamus strateginius tikslus ir uždavinius, analizuoti jų nevykdymo priežastis ir imtis veiksmų situacijai pagerinti.

[172] Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr (Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo, žiūrėta 2022-07-26); https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/faeb5eb4a6c811e9aab6d8dd69c6da66/asr (Dėl Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano patvirtinimo, žiūrėta 2022-07-26).

[173] ITU Guide to Developing a National Cybersecurity Strategy, 2018, 3.2.1 pp.

[174] 2020 m. KAM pradėjo rengti Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano pakeitimo projektą, kuriuo siekta patikslinti trejų metų (2021–2023 m.) laikotarpio Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano priemones, joms įgyvendinti planuojamas lėšas, vertinimo kriterijus ir jų reikšmes, tačiau rengimas buvo sustabdytas, remiantis Vyriausybės išaiškinimu ir Finansų ministerijos pastabomis. Projekto rengimo metu KAM inicijavo raštus (adresuotus institucijoms pagal Strategijos tikslus ir institucijų veiklos sritis) suinteresuotoms institucijoms dėl Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano 2021–2023 metams projekto rengimo. Atsakymus su pasiūlymais pateikė 17 institucijų, su kuriomis buvo derinamas parengtas projektas.

REKOMENDACIJŲ ĮGYVENDINIMO PLANAS

Laukiamas audito poveikis: įgyvendinus rekomendacijas nacionaliniu lygiu bus valdomos informacinių technologijų saugumo rizikos (įskaitant kibernetines), bus sudarytos sąlygos skaitmenizuotai vykdyti kibernetinio saugumo ir IT saugos atitikties vertinimą ir stebėseną. Sklandesnis komunikavimas apie kibernetinius incidentus, sistemingas kibernetinio saugumo subjektų kompetencijų stiprinimas, tipinio kibernetinių incidentų valdymo plano patvirtinimas prisidės prie rezultatyvesnio kibernetinio incidentų suvaldymo.

Pagrindinis audito rezultatas	Rekomendacija (pokytis, kurio siekiama) / priemonės	Pokyčio vertinimo rodikliai ir jų reikšmės*			Subjektas, kuriam pateikta rekomendacija/ įgyvendinantis priemones	Rekomendacijos (pokyčio, kurio siekiama)** / priemonių*** įgyvendinimo terminas
		rodiklis	pradinė reikšmė	siektina reikšmė		
1-asis pagrindinis audito rezultatas Tobulintinas kibernetinio saugumo rizikų valdymas. Nacionaliniu lygiu nekaupiama informacija apie kibernetinio saugumo subjektų identifikuotas ryšių ir informacinių sistemų rizikas, 56 proc. vertinimus atlikusių kibernetinio saugumo subjektų informacijos apie identifikuotas kibernetinio saugumo rizikas Nacionaliniam kibernetinio saugumo centrui nepateikia. Nėra sudarytas nacionalinių kibernetinio saugumo rizikų valdymo priemonių planas, nenustatyta priimtina nacionalinė kibernetinio saugumo rizika, jos tolerancijos ribos.	**Didelės svarbos** 1. Siekiant užtikrinti kibernetinės apsaugos, prevencijos ir atsako priemonių panaudojimą, turi būti diegiamas ir nacionaliniu mastu koordinuojamas informacinių technologijų saugumo rizikų (įskaitant kibernetines) valdymo procesas, kuris leistų gautą informaciją apie kibernetinio saugumo rizikingumo būklę naudoti priimant strateginius sprendimus dėl kibernetinio saugumo stiprinimo.	Nacionalinei stebėsenos sistemai IT saugumo rizikos vertinimus pateikusių valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų ir ypatingos svarbos informacinės infrastruktūros valdytojų dalis	nežinoma	100 proc.	Krašto apsaugos ministerija	2028-12-31
		NKSC atliktų atitikties saugumo reikalavimams, taikomiems valstybės informacinių išteklių valdytojams ir (arba) tvarkytojams ir ypatingos svarbos informacinės infrastruktūros valdytojams, vertinimų dalis	nežinoma	70 proc.		
		Sudarytas ir kasmet atnaujinamas nacionalinis kibernetinio saugumo rizikos profilis	nesudarytas	sudarytas ir kasmet atnaujinamas		
	1.1. Nustatyti Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše reikalavimą valstybės informacinių išteklių valdytojams ir (arba) tvarkytojams, ypatingos				Krašto apsaugos ministerija	2024-12-31

Pagrindinis audito rezultatas	Rekomendacija (pokytis, kurio siekiama) / priemonės	Pokyčio vertinimo rodikliai ir jų reikšmės*			Subjektas, kuriam pateikta rekomendacija / įgyvendinantis priemones	Rekomendacijos (pokyčio, kurio siekiama)** / priemonių*** įgyvendinimo terminas
		rodiklis	pradinė reikšmė	siektina reikšmė		
	svarbos informacinės infrastruktūros valdytojams teikti atliktų ryšių ir informacinių sistemų rizikos vertinimų ataskaitas nacionalinei stebėsenos sistemai.					
	1.2. Remiantis nacionalinei stebėsenos sistemai pateiktais ryšių ir informacinių sistemų rizikos vertinimų duomenimis, atlikti nacionalinio lygio kibernetinio saugumo rizikų vertinimą ir analizę, sudaryti sektorių rizikos profilius.				Nacionalinis kibernetinio saugumo centras	2027-12-31
1-asis pagrindinis audito rezultatas Nesudarytos sąlygos skaitmenizuotai vykdyti saugumo reikalavimų atitiktį ir stebėseną. Ne visais atvejais valstybės informacinių išteklių valdytojai ir (arba) tvarkytojai atlieka atitikties teisės aktų nustatytiems elektroninės informacijos saugos reikalavimams vertinimus ir teikia šiuos duomenis nacionalinei stebėsenos sistemai (ARSIS); kibernetinio saugumo subjektams nesudaryta galimybė ARSIS priemonėmis atlikti vertinimą dėl atitikties kibernetinio saugumo reikalavimams. Nesudarytos galimybės centralizuotai valdyti informaciją apie IT saugos neatitiktis.	**Didelės svarbos** 2. Siekiant kibernetinio saugumo subjektams efektyviau įgyvendinti teisės aktuose nustatytus saugumo reikalavimus, sukurti bendrą kibernetinio saugumo ir informacinių išteklių IT saugos atitikties vertinimo metodiką, sudarančią galimybes atlikti išsamų atitikties teisės aktuose nustatytiems reikalavimams vertinimą ir leisiančią priežiūrą bei stebėseną atliekančiai institucijai rezultatyviau pateikti duomenimis grįstą faktinės būklės nacionalinio lygiu analizę, įžvalgas, apibendrinimą.	Nacionalinei stebėsenos sistemai IT saugumo rizikos vertinimus pateikusių valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų ir ypatingos svarbos informacinės infrastruktūros valdytojų dalis	0 proc.	100 proc.	Krašto apsaugos ministerija	2028-12-31
		Nacionalinės stebėsenos sistemos priemonėmis atliktų valstybės informacinių išteklių IT saugumo atitikties vertinimų dalis	nežinoma	100 proc.		
		NKSC atliktų atitikties saugumo reikalavimams, taikomiems valstybės informacinių išteklių valdytojams ir (arba) tvarkytojams ir ypatingos svarbos informacinės infrastruktūros valdytojams, įvertinimų dalis	nežinoma	70 proc.		
	2.1. Sukurti bendrą kibernetinio saugumo ir informacinių išteklių IT saugos atitikties vertinimo metodiką.				Krašto apsaugos ministerija, Nacionalinis kibernetinio saugumo centras	2026-12-31
	2.2. Sukurti bendrą elektroninės informacijos saugos ir kibernetinio saugumo stebėsenos sistemą:				Nacionalinis kibernetinio saugumo centras	2027-12-31

Pagrindinis audito rezultatas	Rekomendacija (pokytis, kurio siekiama) / priemonės	Pokyčio vertinimo rodikliai ir jų reikšmės*			Subjektas, kuriam pateikta rekomendacija / įgyvendinantis priemones	Rekomendacijos (pokyčio, kurio siekiama)** / priemonių*** įgyvendinimo terminas
		rodiklis	pradinė reikšmė	siektina reikšmė		
	2.2.1. Parengti organizacinių ir techninių saugumo reikalavimų nacionalinės stebėsenos sistemos skaitmenino sprendimo įgyvendinimo modelio sukūrimo ir įdiegimo galimybių studiją.				Nacionalinis kibernetinio saugumo centras	2024-12-31
	2.2.2. Įsigyti, išvystyti ir įdiegti aparatinę ir (arba) programinę įrangą, skirtą skaitmeniniam organizacinių ir techninių saugumo reikalavimų stebėsenos sprendimui įgyvendinti.				Nacionalinis kibernetinio saugumo centras	2026-12-31
	2.2.3. Sukurti ir įdiegti organizacinių ir techninių saugumo reikalavimų nacionalinės stebėsenos sistemos skaitmeninį sprendimą.				Nacionalinis kibernetinio saugumo centras	2027-12-31
2-asis pagrindinis audito rezultatas Tobulintinas kibernetinių incidentų valdymas: - ne visais atvejais kibernetinius incidentus valdančios ir (ar) tiriančios institucijos keičiasi informacija apie kibernetinius incidentus. Kibernetinio saugumo informacinis tinklas neveikia efektyviai ir galėtų būti plačiau pritaikytas naudojimui; - ne visi kibernetinio saugumo subjektai reguliariai dalyvauja kibernetinio saugumo pratybose ir mokymuose, neparengtas tipinis kibernetinių incidentų valdymo planas, ne visi kibernetinio saugumo subjektai turi kibernetinių	**Vidutinės svarbos** 3. Siekiant sudaryti sąlygas, kad visi kibernetinio saugumo subjektai žinotų veiksmus, kurių reikia imtis įvykus kibernetiniam incidentui ar siekiant užkirsti kelią galimoms grėsmėms: - patvirtinti priemones, kurios užtikrintų sklandesnį komunikavimą apie kibernetinius incidentus naudojantis kibernetinio saugumo informaciniu tinklu; - įpareigoti kibernetinio saugumo subjektus (valstybės informacinių išteklių valdytojus ir tvarkytojus) dalyvauti nacionalinėse kibernetinio saugumo pratybose ir numatyti Nacionalinio kibernetinio saugumo centro vykdomos švietimo veiklos vertinimo rodiklius ir juos periodiškai stebėti; - parengti ir patvirtinti detalų tipinį kibernetinių incidentų valdymo planą ir įpareigoti kibernetinio saugumo subjektus pagal šio standartinio plano pavyzdį parengti	Kibernetinio saugumo subjektų, besinaudojančių kibernetiniu saugumo informaciniu tinklu, dalis	41 proc.	100 proc.	Krašto apsaugos ministerija	2025-12-31
		Nacionalinėse kibernetinio saugumo pratybose dalyvavusių valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų ir ypatingos svarbos informacinės infrastruktūros valdytojų dalis	nežinoma	100 proc.		
		Kibernetinių incidentų valdymo planus parengusių valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų ir ypatingos svarbos informacinės infrastruktūros valdytojų dalis	26 proc.	100 proc.		

Pagrindinis audito rezultatas	Rekomendacija (pokytis, kurio siekiama) / priemonės	Pokyčio vertinimo rodikliai ir jų reikšmės*			Subjektas, kuriam pateikta rekomendacija / įgyvendinantis priemones	Rekomendacijos (pokyčio, kurio siekiama)** / priemonių*** įgyvendinimo terminas
		rodiklis	pradinė reikšmė	siektina reikšmė		
incidentų valdymo planą (tvarką).	ar atnaujinti savo vidinius kibernetinių incidentų valdymo planus / tvarkas.					
	3.1. Išvystyti Kibernetinio saugumo informacinio tinklą į naujos kartos tinklą:				Nacionalinis kibernetinio saugumo centras	2023-12-01
	3.1.1. Atlikti analizę ir nustatyti papildomų paslaugų poreikį kibernetinio saugumo subjektams, siekiant išplėsti Kibernetinio saugumo informacinio tinklo paslaugas ir padidinti jo prieinamumą;				Nacionalinis kibernetinio saugumo centras	2023-12-01
	3.1.2. Kibernetinio saugumo subjektams suteikti prieigą prie jų infrastruktūroje įdiegtų kibernetinio saugumo priemonių generuojamų duomenų, taip subjektams suteikiant naudą ir sukuriant paskatas naudotis Kibernetinio saugumo informaciniu tinklu.				Nacionalinis kibernetinio saugumo centras	2023-12-01
	3.2. Nacionalinio kibernetinio saugumo centro strateginiame veiklos plane įvardinti vykdomą švietimo veiklą; šios veiklos vertinimo rodiklius nustatyti centro veiklos plane.				Nacionalinis kibernetinio saugumo centras	2023-03-01
	3.3. Parengti ir patvirtinti tipinį kibernetinių incidentų valdymo planą.				Krašto apsaugos ministerija, Nacionalinis kibernetinio saugumo centras	2023-06-30
	3.4. Patvirtinus tipinį kibernetinių incidentų valdymo planą, pateikti kibernetinio saugumo subjektams nurodymus įgyvendinti plano nuostatas ir įpareigoti juos ne vėliau kaip per 12 mėn. pasirengti kibernetinių incidentų valdymo planus.				Nacionalinis kibernetinio saugumo centras	2023-12-31
	3.5. Nustatyti valstybės informacinių išteklių valdytojams ir (arba) tvarkytojams prievolę dalyvauti nacionalinėse kibernetinio saugumo pratybose.				Krašto apsaugos ministerija	2024-12-31
	3.6. Įvertinti galimybes įpareigoti ypatingos svarbos informacinės infrastruktūros valdytojus dalyvauti nacionalinėse kibernetinio saugumo pratybose.				Nacionalinis kibernetinio saugumo centras	2024-12-31

* Detalūs pokyčių vertinimo rodyklių duomenys pateikti 3 priede „Pokyčių vertinimo rodiklių duomenys“.

** Priemones ir terminus joms įgyvendinti, pokyčiui pasiekti ir rodikliams pamatuoti pateikė Krašto apsaugos ministerija ir Nacionalinis kibernetinio saugumo centras.

*** Rekomendacijų įgyvendinimo stebėsenos metu gali būti tikslinamos arba keičiamos rekomendacijų įgyvendinimo plane nurodytos priemonės ar pokyčių vertinimo rodikliai Valstybinio audito rekomendacijų įgyvendinimo stebėsenos tvarkos aprašo nustatyta tvarka. Aktualus priemonių ir pokyčių vertinimo rodiklių sąrašas yra pateikiamas Valstybės kontrolės atviruose duomenyse adresu www.valstybeskontrole.lt.

Pagrindinis audito rezultatas	Rekomendacija (pokytis, kurio siekiama) / priemonės	Pokyčio vertinimo rodikliai ir jų reikšmės*			Subjektas, kuriam pateikta rekomendacija/ įgyvendinantis priemones	Rekomendacijos (pokyčio, kurio siekiama)** / priemonių*** įgyvendinimo terminas
		rodiklis	pradinė reikšmė	siektina reikšmė		

Atstovas ryšiams, atsakingas už Valstybės kontrolės informavimą apie priemonių įgyvendinimą ir kai kurių rodiklių reikšmes plane nustatytais terminais:

Krašto apsaugos ministerijos Kibernetinio saugumo ir informacinių technologijų politikos grupės vadovas Antanas Aleknavičius, mob. 8 706 80 800, el. p. Antanas.Aleknavicius@kam.lt.

Nacionalinio kibernetinio saugumo centro Informacijos saugumo departamento direktorė Aida Čipkuvienė, mob. 8 706 84 110, el. p. aida.cipkuviene@nksc.lt.

Informacinių technologijų audito departamento vadovas — Markas Marcinkevičius

Informacinių technologijų audito departamento vyriausioji valstybinė auditorė-audito grupės vadovė — Diana Nikitina

PRIEDAI

Valstybinio audito ataskaitos
„Kibernetinio saugumo
užtikrinimas“
1 priedas

Santrumpos ir sąvokos

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

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

CMMI institutas – ISACA dukterinė įmonė, kuri vadovauja mokymosi ir tobulinimo vertinimo procesų lygmeniu programai

CSIRT (angl. *Computer Security Incident Response Team*) – reagavimo į kompiuterinio saugumo incidentus tarnyba

ENISA (angl. *European Union Agency for Cybersecurity*) – Europos Sąjungos kibernetinio saugumo agentūra

ES – Europos Sąjunga

IRD – Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos

IS (informacinė sistema) – valstybės registras, žinybinis registras, valstybės informacinė sistema ir kita informacinė sistema, kurią steigia, kuria ir (arba) tvarko valstybės institucijos, valstybės įstaigos, valstybės įmonės, viešosios įstaigos

ISACA – pirmaujanti pasaulinė asociacija, skleidžianti žinias, išduodanti sertifikatus, vienijanti bendruomenę ir užsiimanti švietimu informacinių sistemų kokybės užtikrinimo ir saugos, organizacijos IT valdymo ir vadovavimo, su IT susijusios rizikos ir atitikties srityse, ne pelno siekianti pasaulinė asociacija, teikianti praktines gaires, standartus ir kitas efektyvias priemones informacinių sistemų naudojimui

YSII – ypatingos svarbos informacinė infrastruktūra

YSVII – ypatingos svarbos valstybės informaciniai ištekliai

IT – Informacinės technologijos

ITU (angl. *International Telecommunication Union*) – Tarptautinė telekomunikacijų sąjunga

KAM – Krašto apsaugos ministerija

Kibernetinio saugumo subjektas (subjektas) – subjektas, valdantis ir (arba) tvarkantis valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojas

KIVT institucija (-os) – kibernetinius incidentus valdanti (-čios) ir (ar) tirianti (-čios) institucija (-os)

KSIT – Kibernetinio saugumo informacinis tinklas

LKPB – Lietuvos kriminalinės policijos biuras

LP – Lietuvos policija

NKSC – Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos

RRT – Ryšių reguliavimo tarnyba

Strategija – Nacionalinė kibernetinio saugumo strategija

ŠMSM – Švietimo, mokslo ir sporto ministerija

TAAIS – Tarptautinis aukščiausiųjų audito institucijų standartas

Tarpinstitucinis veiklos planas – Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas

TM – Teisingumo ministerija

URM – Užsienio reikalų ministerija

VII – valstybės informaciniai ištekliai

VDAI – Valstybinė duomenų apsaugos inspekcija

VRM – Vidaus reikalų ministerija

Asignavimai – valstybės biudžeto ir savivaldybių biudžetų finansinių rodiklių patvirtinimo įstatyme nustatyta lėšų suma, kurią asignavimų valdytojas turi teisę gauti iš biudžete sukauptų lėšų, pateikęs paraišką Valstybės iždą tvarkančiai institucijai arba savivaldybių administracijai, patvirtintoms programoms finansuoti[175]

Bazinė praktika (angl. *Base Practice*) – veikla, kuria, jeigu ji vykdoma nuolatos, prisidedama prie tam tikro proceso tikslo pasiekimo[176]

Efektyvumas – efektyvumo principas reiškia maksimalų turimų išteklių panaudojimą. Čia svarbiausia – naudojamų išteklių ir gaminamo produkto ar paslaugos (kiekio, kokybės ir laiko požiūriu) santykis[177]

[175] Biudžetinės sandaros įstatymas, 2 str. 3 d.

[176] Procesų vertinimo modelis, naudojant COBIT®5, 9 psl.

[177] 300-asis TAAIS „Veiklos audito principai“, 9 psl.

Elektroninė informacija – duomenys, dokumentai ir informacija, tvarkomi valstybės registruose, žinybiniuose registruose, valstybės informacinėse sistemose ir kitose informacinėse sistemose, kurias steigia, kuria ir (arba) tvarko valstybės institucijos, valstybės įstaigos, valstybės įmonės, viešosios įstaigos[178]

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[179]

Kibernetinė erdvė – aplinka, kurią sudaro kompiuteriai ir kita ryšių ir informacinių technologijų įranga ir juose sukuriama ir (arba) jais perduodama elektroninė informacija[180]

Kibernetinė grėsmė – galima aplinkybė, įvykis arba veiksmas, kuris galėtų pažeisti, sutrikdyti arba kitaip neigiamai paveikti tinklų ir informacines sistemas, tokių sistemų naudotojus ir kitus asmenis[181]

Kibernetinis incidentas (incidentas) – įvykis, turintis faktinį neigiamą poveikį tinklų ir informacinių sistemų saugumui[182]. Pagal Kibernetinio saugumo įstatymą – tai 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[183]

Kibernetinių incidentų valdymas (incidentų valdymas) – visos procedūros, padedančios nustatyti, ištirti bei suvaldyti incidentą ir į jį reaguoti[184]. Pagal Kibernetinio saugumo įstatymą - tai procedūros, kurių tikslas – aptikti, analizuoti kibernetinius incidentus ir reaguoti į juos, taip pat atkurti įprastinę ryšių ir informacinių sistemų veiklą[185]

Kibernetinis saugumas – visa veikla, būtina tinklų ir informacinėms sistemoms, tokių sistemų naudotojams ir kitiems susijusiems asmenims apsaugoti nuo kibernetinių grėsmių[186] (taip pat žr. 10 psl.)

Kibernetinio saugumo subjektas (subjektas) – subjektas, valdantis ir (arba) tvarkantis valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros

[178] Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintas Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, 4.1 pp.

[179] Kibernetinio saugumo įstatymas, 2 str. 4 d.

[180] Ten pat, 2 str. 6 d.

[181] Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 2019-04-17 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas), 2 str. 8 p.

[182] Ten pat, 2 str. 6 p.

[183] Kibernetinio saugumo įstatymas, 2 str. 9 d.

[184] Kibernetinio saugumo aktas, 2 str. 7 p.

[185] Kibernetinio saugumo įstatymas, 2 str. 11 d.

[186] Kibernetinio saugumo aktas, 2 str. 1 p.

valdytojas, viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjas[187]

Kibernetinio saugumo taryba – nuolatinė kolegiali nepriklausoma patariamoji institucija, analizuojanti kibernetinio saugumo užtikrinimo būklę Lietuvos Respublikoje ir teikianti kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijoms, kibernetinio saugumo subjektams, mokslo ir studijų institucijoms ir informacinių technologijų srityje veiklą vykdantiems verslo subjektams pasiūlymus dėl kibernetinio saugumo užtikrinimo būklės gerinimo[188]

Registras – teisinių, organizacinių, techninių ir programinių priemonių visuma, skirta registro objektui registruoti ir registro duomenims, registro informacijai, registrui pateiktiems dokumentams ir (arba) jų kopijoms tvarkyti ir naudoti[189]

Rezultatyvumas – rezultatyvumo principas reiškia, kad bus pasiekti iškelti tikslai ir numatyti rezultatai[190]

Rizika – pagrįstai nustatoma aplinkybė ar įvykis, galintis turėti neigiamą poveikį ryšių ir informacinių sistemų saugumui[191]

Rizikų profilis – žinomos rizikos, jos atributų, įskaitant tikėtiną dažnumą, potencialų poveikį ir reagavimo būdus, ir susijusių išteklių, gebos bei esamų kontrolės priemonių aprašas[192]

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[193]

Valstybės informacinė sistema – valstybės institucijai (institucijoms) ar valstybės įstaigai (įstaigoms) teisės aktų nustatytoms funkcijoms, išskyrus vidaus administravimą, atlikti reikalingą informaciją apdorojanti teisinių, organizacinių, techninių ir programinių priemonių visuma[194]

Valstybės informaciniai ištekliai – informacijos, kurią valdo institucijos, atlikdamos teisės aktų nustatytas funkcijas, apdorojamos informacinių technologijų priemonėmis, ir ją apdorojančių informacinių technologijų priemonių visuma[195]

[187] Kibernetinio saugumo įstatymas, 2 str. 8 d.

[188] Ten pat, 7 str. 1 d.

[189] Valstybės informacinių išteklių valdymo įstatymas, 2 str. 6 d.

[190] 300-asis TAAIS „Veiklos audito principai“, 9 psl.

[191] Kibernetinio saugumo įstatymas, 2 str. 15 d.

[192] Procesų vertinimo modelis, naudojant COBIT®5, 61 psl.

[193] Kibernetinio saugumo įstatymas, 2 str. 14 d.

[194] Valstybės informacinių išteklių valdymo įstatymas, 2 str. 14 d.

[195] Ten pat, 2 str. 17 d.

Valstybinio audito ataskaitos
„Kibernetinio saugumo
užtikrinimas“
2 priedas

Audito apimtis ir metodai

Audito apimtis

Audito tikslas – įvertinti, ar užtikrinamas kibernetinis saugumas.

Pagrindiniai audito klausimai – ar užtikrinamas kibernetinio saugumo rizikų valdymas nacionaliniu lygiu; ar kibernetinio saugumo teisinis reguliavimas ir atitikties teisės aktų nustatytiems reikalavimams vertinimo sistema veiksminga; ar užtikrinamas kibernetinių incidentų valdymas; ar užtikrinamas nuoseklus kibernetinio saugumo planavimo įgyvendinimas.

Audituojami subjektai – Krašto apsaugos ministerija, Nacionalinis kibernetinio saugumo centras.

Audituojamas laikotarpis – 2019–2021 m. Siekdami įvertinti tendencijas ir pokyčius, kai kuriais atvejais naudojome ankstesnių (2015–2018 m.) ir 2022 m. duomenis.

Auditas atliktas pagal tarptautinius aukščiausiųjų audito institucijų standartus[196].

Audito duomenų rinkimo ir vertinimo metodai

Audito ataskaitos skyrius / poskyris	Taikyti duomenų rinkimo ir vertinimo metodai	Tikslas
1.1. *Tobulintinas nacionalinis kibernetinio saugumo rizikos valdymas*	<u>*Dokumentų peržiūra*</u> *Nagrinėjome:* ● Nacionalinę kibernetinio saugumo strategiją; ● 2019–2021 m. nacionalines kibernetinio saugumo būklės ataskaitas; ● ENISA gerąją praktiką: nacionalinio lygio rizikos vertinimas, nacionalinės kibernetinio saugumo strategijos rengimas; ● Nacionalinę rizikos analizės ataskaitą; ● Rizikos analizės vadovą; ● Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašą; ● Bendrųjų elektroninės informacijos saugos reikalavimų aprašą. <u>*Duomenų analizė*</u>	*Įvertinti, ar užtikrinamas kibernetinio saugumo rizikos valdymas nacionaliniu lygiu*

[196] 3000-asis TAAIS „Veiklos audito standartas“, prieiga per internetą: https://www.valstybeskontrole.lt/LT/post/15649/ (žiūrėta 2022-09-12).

Audito ataskaitos skyrius / poskyris		Taikyti duomenų rinkimo ir vertinimo metodai	Tikslas
		Analizavome NKSC pateiktą informaciją apie kibernetinio saugumo rizikos valdymą nacionaliniu lygiu. *Apklausa* Apklausėme 231 valstybės informacinių išteklių valdytoją ir (arba) tvarkytoją bei ypatingos svarbos informacinės infrastruktūros valdytoją, 212 atsakymus pateikė. *Pokalbiai* Organizavome pokalbius su KAM, NKSC, IRD, VDAI atstovais.	
1.2.	*Nesudarytos sąlygos skaitmenizuotai vykdyti saugumo reikalavimų atitiktį ir stebėseną*	*Dokumentų peržiūra* *Nagrinėjome:* ● ARSIS nuostatus; ● NKSC nuostatus; ● Kibernetinio saugumo tarybos posėdžio protokolus; ● Organizacinių ir techninių kibernetinio saugumo reikalavimų struktūros ir nuostatų projektą; ● Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašą; ● Bendrųjų elektroninės informacijos saugos reikalavimų aprašą. *Duomenų analizė* *Analizavome:* ● NKSC pateiktą informaciją apie 2019–2021 m. valstybės informacinių sistemų, valstybės ir žinybinių registrų valdytojų ir (ar) tvarkytojų teiktas informacinių technologijų saugos atitikties vertinimo ataskaitas; ● NKSC pateiktą informaciją apie ARSIS funkcionalumus; ● KAM pateiktą informaciją apie organizacinių ir techninių kibernetinio saugumo reikalavimų struktūros ir nuostatų projektą. *Apklausa* Apklausėme 176 valstybės informacinių išteklių valdytojus ir (arba) tvarkytojus. *Pokalbiai* Organizavome pokalbius su KAM, NKSC, IRD, VDAI atstovais.	*Įvertinti, ar ARSIS užtikrina atitikties teisės aktų nustatytiems kibernetinio saugumo reikalavimams vertinimą*
1.3.	*Dar nėra konsoliduotas kibernetinio saugumo ir elektroninės informacijos saugos teisinis reguliavimas*	*Dokumentų peržiūra* *Nagrinėjome:* ● Kibernetinio saugumo įstatymą;	*Įvertinti, ar kibernetinio saugumo teisinis reguliavimas yra veiksmingas*

Audito ataskaitos skyrius / poskyris	Taikyti duomenų rinkimo ir vertinimo metodai	Tikslas
	• Valstybės informacinių išteklių valdymo įstatymą; • Administracinės naštos mažinimo įstatymą; • Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašą; • Bendrųjų elektroninės informacijos saugos reikalavimų aprašą; • Saugos dokumentų turinio gairių aprašą; • Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašą; • ITU pasaulinius kibernetinio saugumo indeksus ir jų vertinimo metodologiją. • Veiklos audito „Kibernetinio saugumo aplinka Lietuvoje“ rekomendacijų įgyvendinimo būklę. *Duomenų analizė* Analizavome KAM pateiktą rengiamos naujos kibernetinio saugumo reikalavimų sistemos[197] projektą. *Apklausa* Apklausėme 231 valstybės informacinių išteklių valdytoją ir (arba) tvarkytoją bei ypatingos svarbos informacinės infrastruktūros valdytoją, iš jų 212 pateikė atsakymus. *Pokalbiai* • Organizavome pokalbius su KAM, NKSC, IRD, VDAI atstovais.	
2.1. Apie kibernetinius incidentus turi būti komunikuojama sklandžiau	*Dokumentų peržiūra* *Nagrinėjome:* • Nacionalinį kibernetinių incidentų valdymo planą; • Kibernetinio saugumo įstatymą; • NKSC nuostatus; • ES Tarybos „Europos kibernetinių nusikaltimų prevencijos ir kovos su tokiais nusikaltimais politikos praktinis įgyvendinimas ir veikimas“ įvertinimo ataskaitą apie Lietuvą; • Nacionalinę kibernetinio saugumo būklės 2020 m. ataskaitą;	*Įvertinti, ar sklandus komunikavimas apie kibernetinius incidentus*

[197] 2021-03-02 pristatyta Kibernetinio saugumo tarybos posėdyje.

Audito ataskaitos skyrius / poskyris	Taikyti duomenų rinkimo ir vertinimo metodai	Tikslas
	• ENISA gerąją praktiką: CSIRT ir teisėsaugos institucijų bendradarbiavimas kovojant su elektroniniais nusikaltimais. <u>*Duomenų analizė*</u> *Analizavome:* • NKSC pateiktą informaciją apie gautus pranešimus apie kibernetinius incidentus ir informacijos perdavimą LP, VDAI; • VDAI pateiktą informaciją apie inspekcijos gautus pranešimus apie asmens duomenų saugumo pažeidimus ir informacijos perdavimą NKSC, LP; • LP pateiktą informaciją apie gautus pranešimus apie incidentus, galimai nusikaltimus ir informacijos perdavimą NKSC, VDAI; • NKSC pateiktą informaciją apie KSIT naudojimą. <u>*Apklausa*</u> Apklausėme 231 valstybės informacinių išteklių valdytoją ir (arba) tvarkytoją bei ypatingos svarbos informacinės infrastruktūros valdytoją, 212 atsakymus pateikė. <u>*Pokalbiai*</u> Organizavome pokalbius su KAM, NKSC, LP, VDAI, IRD, RRT atstovais.	
2.2. Kibernetinio saugumo pratybos, mokymai ir konsultacijos vykdomos, tačiau yra nepakankamos siekiant stiprinti subjektų gebėjimus suvaldyti kibernetinius incidentus	<u>*Dokumentų peržiūra*</u> *Nagrinėjome:* • Kibernetinio saugumo įstatymą; • Nacionalinė kibernetinio saugumo strategiją; • Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinį veiklos planą; • Nacionalinį kibernetinių incidentų valdymo planą; • NKSC nuostatus; • Tipinį kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planą (galiojo iki 2018-12-31). <u>*Duomenų analizė*</u> *Analizavome:* • 2019–2021 m. nacionalinių kibernetinio saugumo pratybų „Kibernetinis skydas“ ataskaitas; • KAM ir NKSC pateiktą informaciją apie kibernetinio saugumo pratybų ir mokymų rengimą,	*Įvertinti, ar KAM ir NKSC vykdoma veikla prisideda prie tinkamo kibernetinio saugumo subjektų gebėjimų suvaldyti kibernetinius incidentus tobulinimo*

Audito ataskaitos skyrius / poskyris	Taikyti duomenų rinkimo ir vertinimo metodai	Tikslas
	teiktas konsultacijas ir metodinę pagalbą; ● KAM informaciją apie tipinio kibernetinių incidentų valdymo plano parengimą. *Apklausa* Apklausėme 231 valstybės informacinių išteklių valdytoją ir (arba) tvarkytoją bei ypatingos svarbos informacinės infrastruktūros valdytoją, iš jų 212 atsakymus pateikė. *Pokalbiai* Organizavome pokalbius su KAM, NKSC atstovais.	
3. Neužtikrinamas nuoseklus kibernetinio saugumo planavimo įgyvendinimas	*Dokumentų peržiūra* *Nagrinėjome:* ● Strateginio valdymo įstatymą; ● Aštuonioliktosios Lietuvos Respublikos Vyriausybės programos nuostatų įgyvendinimo planą; ● Strateginio planavimo metodiką; ● Nacionalinė kibernetinio saugumo strategiją; ● Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinį veiklos planą; ● Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano pakeitimo projektą[198]. *Duomenų analizė* *Analizavome:* ● 2019 ir 2020 m. Nacionalinės kibernetinio saugumo strategijos įgyvendinimo ataskaitas; ● KAM, VRM, TM, URM, ŠMSM, RRT pateiktą informaciją apie Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinį veiklos plano priemonių vykdymą 2021 m. *Pokalbiai* Organizavome pokalbius su KAM, NKSC atstovais.	*Įvertinti, ar pasiekti nacionalinių kibernetinio saugumo planavimo dokumentuose suplanuoti rezultatai.*

[198] Vyriausybės 2020-11-24 nutarimo „Dėl Vyriausybės 2019-07-03 nutarimo Nr. 709 „Dėl Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano patvirtinimo“ pakeitimo“ projektas Nr. 20-8431 (registruotas 2020-06-11; žiūrėta 2022-06-29).

Valstybinio audito ataskaitos
„Kibernetinio saugumo užtikrinimas“
3 priedas

Pokyčių vertinimo rodiklių duomenys

Rodiklis		Nacionalinei stebėsenos sistemai IT saugumo rizikos vertinimus pateikusių valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų ir ypatingos svarbos informacinės infrastruktūros valdytojų dalis	Nacionalinės stebėsenos sistemos priemonėmis atliktų valstybės informacinių išteklių IT saugumo atitikties vertinimų dalis	NKSC atliktų atitikties saugumo reikalavimams, taikomiems valstybės informacinių išteklių valdytojams ir tvarkytojams, ypatingos svarbos informacinės infrastruktūros valdytojams, įvertinimų dalis	Sudarytas ir kasmet atnaujinamas nacionalinis kibernetinio saugumo rizikos profilis	Nacionalinėse kibernetinio saugumo pratybose dalyvavusių valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų ir ypatingos svarbos informacinės infrastruktūros valdytojų dalis	Kibernetinių incidentų valdymo planus parengusių valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų ir ypatingos svarbos informacinės infrastruktūros valdytojų dalis	Kibernetinio saugumo subjektų, besinaudojančių kibernetiniu saugumo informaciniu tinklu, dalis
Matavimo vienetas		Proc.	Proc.	Proc.		Proc.	Proc.	Proc.
Pradinė reikšmė		nežinoma	nežinoma	nežinoma	nesudarytas	nežinoma	26	41
Pradinės reikšmės fiksavimo data		2021 m.	2021 m.	2021 m.	2022 m.	2021 m.	2022 m.	2021 m.
Siektina reikšmė		100	100	70	sudarytas ir kasmet atnaujinamas	100	100	100
Tolerancijos ribos	Gerai	≥ 85	≥ 85	≥ 60	Sudarytas	≥ 85	≥ 85	≥ 85
	Vidutiniškai	61-84	61-84	41-59	iš dalies sudarytas	61-84	61-84	61-84
	Blogai	≤ 60	≤ 60	≤ 40	nesudarytas	≤ 60	≤ 60	≤ 60
Siektina reikšmė bus fiksuota		2028 m.	2028 m.	2028 m.	2028 m.	2025 m.	2025 m.	2025 m.
Duomenų šaltinis rodikliui skaičiuoti		NKSC duomenys	NKSC duomenys	NKSC duomenys	NKSC duomenys	NKSC duomenys	NKSC duomenys	NKSC duomenys
Periodinės reikšmės fiksavimo data		Vertinant pokytį	Vertinant pokytį	Vertinant pokytį	Vertinant pokytį	Vertinant pokytį	Vertinant pokytį	Kasmet
Detalus skaičiavimo / vertinimo aprašymas		X=a/b*100; a – per metus IT saugumo rizikos vertinimus pateikusių VII valdytojų ir (arba) tvarkytojų, YSVII valdytojų skaičius; b – VII valdytojų ir (arba) tvarkytojų, YSVII valdytojų skaičius	X=a/b*100; a – Nacionalinės stebėsenos sistemos priemonėmis atliktų VII IT saugumo atitikties vertinimų skaičius; b – Valstybės registrų ir informacinių sistemų registre registruotų VII skaičius	X=a/b*100; a – NKSC per metus atliktų atitikties saugumo reikalavimams įvertinimų skaičius; b – VII valdytojų ir (arba) tvarkytojų, YSVII valdytojų per metus pateiktų IT saugumo atitikties vertinimų skaičius	NKSC duomenų analizė	X=a/b*100; a – pratybose dalyvavusių VII valdytojų ir (arba) tvarkytojų, YSVII valdytojų skaičius; b – VII valdytojų ir (arba) tvarkytojų, YSVII valdytojų skaičius	X=a/b*100; a – kibernetinių incidentų valdymo planus parengusių VII valdytojų ir (arba) tvarkytojų, YSVII valdytojų skaičius; b – VII valdytojų ir (arba) tvarkytojų, YSVII valdytojų skaičius	X=a/b*100; a – prisijungusių prie KSIT VII valdytojų ir (arba) tvarkytojų, YSVII valdytojų skaičius; b – VII valdytojų ir (arba) tvarkytojų, YSVII valdytojų skaičius

Elektroninės informacijos saugos ir kibernetinio saugumo reikalavimų tapatumo pavyzdžiai

LST EN ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“	Elektroninės informacijos saugą nustatantis teisinis reguliavimas	Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas
A.6.2.1 Mobiliųjų įrenginių politika Kontrolės priemonė: siekiant apsisaugoti nuo rizikų, susijusių su mobiliaisiais įrenginiais, turi būti taikoma oficiali politika ir palaikančios saugumo priemonės.	„Saugus elektroninės informacijos tvarkymas“ skyriuje turi būti nurodyta **nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių naudojimo tvarka** (4.3.9 pp.)*	Subjektai, valdantys ir (arba) tvarkantys VII, YSII valdytojai, suderinę su NKSC, tvirtina kibernetinio saugumo politikos ir jos įgyvendinimo **dokumentus, kuriuose turi būti nustatyta mobiliųjų įrenginių,** naudojamų prisijungti prie VII ar YSII, **saugus naudojimas** ir kontrolė (5.3.9 pp.)
	„Organizaciniai ir techniniai reikalavimai“ skyriuje turi būti nurodyti metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą (nurodomas **nuotolinio prisijungimo** prie IS būdas, protokolas, **elektroninės informacijos** keitimosi formatai, **šifravimo**, elektroninės informacijos kopijų skaičiaus **reikalavimai** <...>) (3.3.5 pp.)*	Subjektai, valdantys ir (arba) tvarkantys VII, YSII valdytojai, suderinę su NKSC, tvirtina kibernetinio saugumo politikos ir jos įgyvendinimo **dokumentus,** kuriuose **turi būti nustatyti duomenų, esančių mobiliuosiuose įrenginiuose, šifravimo nuostatos** (5.3.10 pp.)
	IS dalys, **atliekančios nutolusio prisijungimo autentikavimą, turi drausti** automatiškai **išsaugoti slaptažodžius** (5.14.4 pp.)*** Reikalavimas taikytinas I, II, III, IV kategorijų IS	VII ar YSII dalys, patvirtinančios VII ar YSII naudotojo tapatumą, **turi drausti išsaugoti slaptažodžius** <...> (Priedo 13.4 pp.) Reikalavimas taikytinas YSII, I, II, III, IV kategorijų VII
A.6.2.2 Nuotolinis darbas Kontrolės priemonė: siekiant apsaugoti nutolusiose vietovėse pasiekiamą, apdorojamą ir saugomą informaciją, turi būti numatyta ir įgyvendinta nuotolinio darbo politika ir ją palaikančios priemonės.	„Organizaciniai ir techniniai reikalavimai“ skyriuje **turi būti nurodytos** leistinos kompiuterių (ypač nešiojamųjų) naudojimo ribos (**jeigu kompiuterius leidžiama naudoti nustatytoms funkcijoms atlikti ne institucijos patalpose, turi būti nurodytos papildomos saugos priemonės** <...> (3.3.4 pp.)*	Subjektai, valdantys ir (arba) tvarkantys VII, YSII valdytojai, suderinę su NKSC, tvirtina kibernetinio **saugumo politikos ir jos įgyvendinimo dokumentus**, kuriuose **turi būti nustatytas** VII ar YSII išteklių **naudojimas už organizacijos ribų ir (arba) mobiliaisiais įrenginiais** (5.3.11 pp.)
	„Saugaus elektroninės informacijos teikimo IS naudotojams kontrolės tvarka“ skyriuje **turi būti nurodyti leistini nuotolinio IS naudotojų prisijungimo prie IS būdai** (6.3.5 pp.)*	
A.7.2.2 Informacijos saugumo supratimas, švietimas ir mokymas Kontrolės priemonė: visi organizacijos darbuotojai ir, kai reikia, rangovai turi būti tinkamai mokomi ir nuolat informuojami apie organizacijos politikos bei procedūrų, susijusių su jų darbu, pokyčius.	Saugos įgaliotinis periodiškai organizuoja IS **naudotojų mokymą elektroninės informacijos saugos klausimais** <...> (25 p.)**	Subjektai, valdantys ir (arba) tvarkantys VII, YSII valdytojai, suderinę su NKSC, tvirtina kibernetinio saugumo politikos ir jos įgyvendinimo dokumentus, kuriuose turi būti **nustatyti** VII ar YSII **naudotojų,** kompetentingo asmens ar padalinio, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, **mokymai kibernetinio saugumo klausimais** (5.3.4 pp.)
A.9.1.1 Prieigos valdymo politika Kontrolės priemonė: vadovaujantis veiklos ir informacijos saugumo reikalavimais turi būti numatyta,	IS valdytojas privalo turėti pagal <...> Vyriausybės patvirtintą Saugos dokumentų turinio gairių aprašą **parengtas** <...> ir **patvirtintas IS naudotojų administravimo taisykles** (7.4 pp.)**	Subjektai, valdantys ir (arba) tvarkantys VII, YSII valdytojai, suderinę su NKSC, **tvirtina** kibernetinio saugumo politikos ir jos įgyvendinimo **dokumentus, kuriuose turi būti nustatytas** VII ar YSII

LST EN ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“	Elektroninės informacijos saugą nustatantis teisinis reguliavimas	Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas
dokumentuota ir peržiūrima prieigos valdymo politika.	„Saugaus elektroninės informacijos teikimo IS naudotojams kontrolės tvarka“ skyriuje **turi būti nurodyta tvarka, kuria bus registruojami ir išregistruojami** IS **naudotojai <...>** (6.3.1 pp.)*	**naudotojų** grupių sudarymas, **teisių ir prieigos prie** VII ar YSII **paslaugų ir išteklių suteikimas ir valdymas** (5.3.2 pp.)
	IS naudotojų administravimo taisyklėse **turi būti nurodyti prieigos prie elektroninės informacijos principai;** IS **naudotojų** įgaliojimai, **teisės** ir pareigos tvarkant elektroninę informaciją (6.1.2; 6.2.1 pp.)*	
A.9.2.3 Prieigos teisių valdymas Kontrolės priemonė: Prieigos teisių paskyrimas ir naudojimasis turi būti apribotas ir valdomas.	IS priežiūros **funkcijos turi būti atliekamos naudojant atskirą tam skirtą IS administratoriaus paskyrą, kuria naudojantis negalima atlikti** IS **naudotojo funkcijos** (5.3 pp.)***	VII ar YSII priežiūrą vykdančio asmens <...> (**administratorius**) **funkcijos turi būti atliekamos naudojant atskirą tam skirtą paskyrą, kuri negali būti naudojama** kasdienėms VII ar YSII **naudotojo funkcijoms atlikti** (Priedo 1 p.)
	Reikalavimas taikytinas I, II, III, IV kategorijų IS	Reikalavimas taikytinas YSII, I, II, III, IV kategorijų VII
	IS **naudotojams negali būti suteikiamos** IS **administratoriaus teisės** (5.4 pp.)***	VII ar YSII **naudotojams negali būti suteikiamos administratoriaus teisės** (Priedo 2 p.)
	Reikalavimas taikytinas I, II, III, IV kategorijų IS	Reikalavimas taikytinas YSII, I, II, III, IV kategorijų VII
	IS **naudotojas** ar IS **administratorius turi patvirtinti savo tapatybę slaptažodžiu arba kita autentiškumo patvirtinimo priemone** (5.7 pp.)***	VII ar YSII **naudotojas** ar **administratorius turi patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone** (Priedo 5 p.)
	Reikalavimas taikytinas I, II, III, IV kategorijų IS	Reikalavimas taikytinas YSII, I, II, III, IV kategorijų VII
A.9.2.4 Slaptos naudotojų autentiškumo patvirtinimo informacijos valdymas Kontrolės priemonė: slaptos naudotojų autentiškumo patvirtinimo informacijos paskyrimas turi būti valdomas vadovaujantis oficialia valdymo procedūra.	**Kiekvienas** IS **naudotojas turi būti** IS **unikaliai identifikuojamas (asmens kodas negali būti naudojamas kaip** IS **naudotojo identifikatorius)** (5.5 pp.)***	**Kiekvienas** VII ar YSII **naudotojas turi būti unikaliai atpažįstamas (asmens kodas negali būti naudojamas** VII ar YSII **naudotojui atpažinti**) (Priedo 3 p.)
	Reikalavimas taikytinas I, II, III, IV kategorijų IS	Reikalavimas taikytinas YSII, I, II, III, IV kategorijų VII
A.9.3.1 Slaptos autentiškumo patvirtinimo informacijos naudojimas Kontrolės priemonė: turi būti reikalaujama laikytis organizacijoje galiojančios tvarkos naudojantis slapta autentiškumo patvirtinimo informacija.	**Draudžiama slaptažodžius atskleisti tretiesiems asmenims** (5.14.3 pp.)***	**Draudžiama slaptažodžius atskleisti kitiems asmenims** (Priedo 13.3 pp.)
	Reikalavimas taikytinas I, II, III, IV kategorijų IS	Reikalavimas taikytinas YSII, I, II, III, IV kategorijų VII
A.9.4.2 Saugiosios prisijungimo procedūros Kontrolės priemonė: ten, kur prieigos valdymo politika reikalauja, prieiga prie sistemų ir taikomųjų programų turi būti valdoma naudojant saugiąją prisijungimo procedūrą.	„Saugaus elektroninės informacijos teikimo IS naudotojams kontrolės tvarka“ skyriuje turi būti nurodyti IS **naudotojų slaptažodžių sudarymo**, galiojimo trukmės ir **keitimo reikalavimai** (6.3.3 pp.)*	Subjektai, valdantys ir (arba) tvarkantys VII, YSII valdytojai, suderinę su NKSC, tvirtina kibernetinio saugumo politikos ir jos įgyvendinimo dokumentus, kuriuose **turi būti nustatyta** VII ar YSII **naudotojų** vardų **ir slaptažodžių sudarymas,** apsauga ir **keitimas** (5.3.5 pp.)
	<...> **turi būti nustatytas didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius, kuris turėtų būti ne didesnis nei 5 kartai;** neteisingai įvedus didžiausią leistiną slaptažodžių skaičių, **IS turi užsirakinti ir neleisti IS naudotojui identifikuotis** IS valdytojo	**Turi būti nustatytas didžiausias leistinas** VII ar YSII **naudotojo mėginimų įvesti teisingą slaptažodį skaičius (ne daugiau kaip penki kartai)** <...>. **Iš eilės neteisingai įvedus slaptažodį tiek kartų, kiek nustatyta,** VII ar YSII naudotojo

LST EN ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“	Elektroninės informacijos saugą nustatantis teisinis reguliavimas	Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas
	tvirtinamose IS naudotojų administravimo taisyklėse **nustatytą laiko tarpą, kuris turi būti ne trumpesnis nei 15 minučių** (5.14.5 pp.)*** Reikalavimas taikytinas I, II, III, IV kategorijų IS	**paskyra turi užsirakinti ir neleisti** VII ar YSII **naudotojui patvirtinti** tapatybės kibernetinio saugumo politikos ir jos įgyvendinimo dokumentuose **nustatytą laiką – ne trumpiau kaip penkiolika minučių** <...> (Priedo 13.5 pp.) Reikalavimas taikytinas II, III, IV kategorijų VII
	Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu <...> **tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jei** IS **naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio; nėra techninių galimybių** IS **naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu** (5.14.6 pp.)*** Reikalavimas taikytinas I, II, III, IV kategorijų IS	**Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu**. <..> **tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo**, jeigu VII ar YSII **naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio** ar **nėra techninių galimybių** VII ar YSII **naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu** (Priedo 13.7 pp.) Reikalavimas taikytinas YSII, I, II, III, IV kategorijų VII
A.9.4.3 Slaptažodžių tvarkymo sistema Kontrolės priemonė: slaptažodžių tvarkymo sistemos turi būti interaktyvios ir užtikrinti kokybiškų slaptažodžių naudojimą.	**Slaptažodis turi būti keičiamas ne rečiau kaip kas 3 mėnesius** (5.14.7.1 pp.)*** Reikalavimas taikytinas I, II, III, IV kategorijų IS	**Slaptažodis turi būti keičiamas ne rečiau kaip kas tris mėnesius** (Priedo 13.8.1 pp.) Reikalavimas taikytinas YSII, I, II, III kategorijų VII
	Slaptažodį turi sudaryti ne mažiau kaip 8 simboliai (5.14.7.2 pp.)*** Reikalavimas taikytinas I, II, III, IV kategorijų IS	**Slaptažodį turi sudaryti ne mažiau kaip aštuoni simboliai** <...> (Priedo 13.8.2 pp.) Reikalavimas taikytinas YSII, I, II, III kategorijų VII
	Keičiant slaptažodį IS **neturi leisti sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių** (5.14.7.3 pp.)*** Reikalavimas taikytinas I, II, III, IV kategorijų IS	**Keičiant slaptažodį,** VII ar YSII **neturi leisti sudaryti slaptažodžio iš buvusių šešių paskutinių slaptažodžių** <...> (Priedo 13.8.3 pp.) Reikalavimas taikytinas YSII, I, II kategorijų VII
	Pirmojo prisijungimo prie IS **metu iš** IS **naudotojo turi būti reikalaujama, kad jis pakeistų slaptažodį** (5.14.7.4 pp.)*** Reikalavimas taikytinas I, II, III, IV kategorijų IS	**Pirmąkart jungiantis** prie VII ar YSII, **turi būti reikalaujama, kad** VII ar YSII **naudotojas pakeistų slaptažodį** <...> (Priedo 13.8.4 pp.) Reikalavimas taikytinas YSII, I, II, III, IV kategorijų VII
	Slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius (5.14.8.1 pp.)*** Reikalavimas taikytinas I, II, III, IV kategorijų IS	**Slaptažodis turi būti keičiamas ne rečiau kaip kas du mėnesius** (Priedo 13.9.1 pp.) Reikalavimas taikytinas YSII, I, II, III kategorijų VII
	Slaptažodį turi sudaryti ne mažiau kaip 12 simbolių (5.14.8.2 pp.)*** Reikalavimas taikytinas I, II, III, IV kategorijų IS	**Slaptažodį turi sudaryti ne mažiau kaip dvylika simbolių** (Priedo 13.9.2 pp.) Reikalavimas taikytinas YSII, I, II, III kategorijų VII
	Keičiant slaptažodį IS taikomoji programinė įranga neturi leisti sudaryti slaptažodžio iš buvusių 3 paskutinių slaptažodžių (5.14.8.3 pp.)*** Reikalavimas taikytinas I, II, III, IV kategorijų IS	**Keičiant slaptažodį, taikomoji programinė įranga neturi leisti sudaryti slaptažodžio iš buvusių trijų paskutinių slaptažodžių** <...> (Priedo 13.9.3 pp.) Reikalavimas taikytinas YSII, I, II, III kategorijų VII

LST EN ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“	Elektroninės informacijos saugą nustatantis teisinis reguliavimas	Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas
A.12.2.1 Apsaugos nuo kenkimo programų kontrolės priemonės Kontrolės priemonė: turi būti įgyvendintos tinkamos aptikimo, išvengimo bei atkūrimo priemonės, skirtos apsisaugoti nuo kenkimo programų, o reikiami naudotojai turi būti su jomis supažindinti.	„Organizaciniai ir techniniai reikalavimai“ skyriuje **turi būti nurodyta programinės įrangos, skirtos apsaugoti IS nuo kenksmingos programinės įrangos** <...> **naudojimo nuostatos** <...> (3.3.1 pp.)*	Subjektai, valdantys ir (arba) tvarkantys VII ar YSII valdytojai, suderinę su NKSC, tvirtina kibernetinio saugumo politikos ir jos įgyvendinimo dokumentus, kuriuose **turi būti nustatytas pažeidžiamumų nustatymo programinės įrangos naudojimas** (5.3.16 pp.)
	IS tarnybinėse stotyse ir vidinių IS naudotojų kompiuteriuose **turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingosios programinės įrangos aptikimo, stebėjimo realiu laiku priemonės** <...> (5.12.3 pp.)***	Mobiliuosiuose įrenginiuose **privalo būti naudojamos centralizuotai valdomos ir atnaujinamos kenkimo programinės įrangos aptikimo,** <...> **stebėjimo priemonės** (Priedo 51 p.)
	Reikalavimas taikytinas I, II, III, IV kategorijų IS	Reikalavimas taikytinas YSII, I kategorijos VII
A.12.4.1 Įvykių registravimas Kontrolės priemonė: turi būti tvarkomi, saugomi ir peržiūrimi naudotojų veiklos, išimčių, trikčių ir informacijos saugumo įvykių žurnalai.	„Saugus elektroninės informacijos tvarkymas“ skyriuje **turi būti nurodyta IS naudotojų veiksmų registravimo tvarka** (4.3.2 pp.)*	Subjektai, valdantys ir (arba) tvarkantys VII, YSII valdytojai, suderinę su NKSC, tvirtina kibernetinio saugumo politikos ir jos įgyvendinimo **dokumentus**, kuriuose **turi būti nustatytas audito įrašų administravimas ir saugojimas** (5.3.6 pp.)
	IS **turi būti įrašomi** ir IS valdytojo tvirtinamose Saugaus elektroninės informacijos tvarkymo taisyklėse nustatytą laiką saugomi duomenys apie IS tarnybinių stočių, IS **taikomosios programinės įrangos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis** IS tarnybinėse stotyse, IS taikomojoje programinėje įrangoje, **visus IS naudotojų vykdomus veiksmus, kitus elektroninės informacijos saugai svarbius įvykius, nurodant** IS naudotojo identifikatorių ir elektroninės informacijos saugai svarbaus **įvykio ar vykdyto veiksmo laiką** <...> (5.2 pp.)*** Reikalavimas taikytinas I, II, III, IV kategorijų IS	Auditui atlikti **turi būti fiksuojamas** VII ar YSII **elementų įjungimas/ išjungimas ar perkrovimas** <...> (Priedo 18.1 pp.) Auditui atlikti **turi būti fiksuojamas** VII ar YSII **naudotojų, administratoriaus prisijungimas (ir nesėkmingi bandymai prisijungti)/ atsijungimas** (Priedo 18.2 pp.) Kiekviename audito duomenų įraše turi būti **fiksuojama įvykio data ir tikslus laikas** <...> (Priedo 21.1 pp.) Reikalavimai taikytini YSII, I, II, III, IV kategorijos VII
A.12.5.1 Programinės įrangos diegimas operacinėse sistemose Kontrolės priemonė: turi būti įgyvendintos procedūros, skirtos programinės įrangos diegimui į operacines sistemas valdyti.	**Turi būti** operatyviai testuojami ir **įdiegiami** IS tarnybinių stočių ir vidinių IS naudotojų darbo vietų kompiuterinės įrangos **operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai** <...> (5.12.4 pp.)*** Reikalavimas taikytinas I, II, III, IV kategorijų IS	**Turi būti įdiegiamos operacinės sistemos ir kiti naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai** (Priedo 52 p.) Reikalavimas taikytinas YSII, I, II, III, IV kategorijos VII
A.13.1.1 Tinklo kontrolės priemonės Kontrolės priemonė: tinklai turi būti tinkamai valdomi ir prižiūrimi, siekiant apsaugoti informaciją sistemose ir taikomosiose programose.	„Techninių ir kitų saugos priemonių aprašymas“ skyriuje turi būti nurodytos **elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės** (4.2.3 pp.)*	Subjektai, valdantys ir (arba) tvarkantys VII, YSII valdytojai, suderinę su NKSC, tvirtina kibernetinio saugumo politikos ir jos įgyvendinimo dokumentus, kuriuose **turi būti nustatytas saugus naudojimasis belaidžiu tinklu** (5.3.8 pp.)

LST EN ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“	Elektroninės informacijos saugą nustatantis teisinis reguliavimas	Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas
	IS programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), XSS (angl. Cross-site scripting), atkirtimo nuo paslaugos (angl. *DOS*), dedikuoto atkirtimo nuo paslaugos (angl. *DDOS*) ir kitų; pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. *The Open Web Application Security Project (OWASP)* interneto svetainėje www.owasp.org (5.12.16 pp.)*** Reikalavimas taikytinas I, II, III, IV kategorijų IS	Turi būti naudojamos apsaugos nuo pagrindinių per tinklą vykdomų atakų: struktūrizuotų užklausų kalbos įskverbties (angl. *SQL injection*), įterptinių instrukcijų atakų (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS*), paskirstyto atsisakymo aptarnauti (angl. *DDOS*) ir kitų, priemonės; pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. *The Open Web Application Security Project (OWASP)*) interneto svetainėje www.owasp.org (Priedo 71 p.) Reikalavimas taikytinas YSII, I, II kategorijų VII
	Pagrindinėse IS tarnybinėse stotyse turi būti įjungtos ugniasienės, sukonfigūruotos praleisti tik su IS funkcionalumu ir administravimu susijusį duomenų srautą <...> (7.12 pp.)*** Reikalavimas taikytinas I, II kategorijų IS	Pagrindinėse tarnybinėse stotyse turi būti įjungtos saugasienės, sukonfigūruotos blokuoti visą įeinantį ir išeinantį, išskyrus su VII ar YSII funkcionalumu ir administravimu susijusį duomenų srautą (Priedo 34 p.) Reikalavimas taikytinas YSII, I, II, III, IV kategorijų VII
	IS tinkle turi būti įdiegtos ir veikti automatinės įsilaužimo aptikimo sistemos (7.13 pp.)*** Reikalavimas taikytinas I, II kategorijų IS	Turi būti įdiegtos ir veikti įsibrovimo aptikimo sistemos, kurios stebėtų VII ar YSII įeinantį ir išeinantį duomenų srautą ir vidinį srautą tarp svarbiausių tinklo paslaugų (Priedo 30 p.) Reikalavimas taikytinas YSII, I, II, III, IV kategorijų VII

* Saugos dokumentų turinio gairių aprašas

** Bendrųjų elektroninės informacijos saugos reikalavimų aprašas

*** Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašas

Šaltinis – Valstybės kontrolė