Valstybinio audito ataskaita

KIBERNETINIO SAUGUMO APLINKA LIETUVOJE

2015 m. gruodžio 9 d. Nr. VA-P-90-4-16

Su valstybinio audito ataskaita galima susipažinti Valstybės kontrolės interneto puslapyje adresu www.vkontrole.lt

TURINYS

SANTRUMPOS IR SĄVOKOS

Vartojamos sąvokos[1]:

Elektroninė informacija – informacinėje sistemoje tvarkomi duomenys, dokumentai ir informacija.

Elektroninės informacijos sauga – elektroninės informacijos konfidencialumo (su tvarkoma elektronine informacija gali susipažinti tik įgalioti asmenys), vientisumo (elektroninė informacija nebuvo atsitiktinai ar neteisėtai pakeista ar sunaikinta) ir prieinamumo (elektroninė informacija gali būti tvarkoma reikiamu metu) užtikrinimas.

Ypatingos svarbos informacinė infrastruktūra – elektroninių ryšių tinklas ar jo dalis, informacinė sistema ar jos dalis, informacinių sistemų grupė ar pramoninių procesų valdymo sistema ar jos dalis, nepaisant to, ar jos valdytojas yra privatus ar viešojo administravimo subjektas, kuriuose įvykęs kibernetinis incidentas gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui, valstybės ir visuomenės interesams.

Kibernetinė erdvė – aplinka, kurioje pavieniuose kompiuteriuose ar kitoje informacinėje ir ryšių technologijų įrangoje sukuriama elektroninė informacija ir (arba) perduodama per elektroninių ryšių tinklu sujungtus kompiuterius ar kitą informacinių ir ryšių technologijų įrangą.

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

Kibernetinis saugumas – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti.

Šioje audito ataskaitoje **kibernetinis saugumas** suprantamas plačiau nei apibrėžia Kibernetinio saugumo įstatymas ir apima taip pat Tarptautinės standartizacijos organizacijos (ISO) standartuose[2] ir Šiaurės Atlanto Sutarties Organizacijos (NATO) Kibernetinės gynybos tobulinimo kompetencijos centro pateiktose rekomendacijose[3] priskiriamus elementus (el. informacijos, taikomųjų programų, tinklų, interneto ir ypatingos svarbos informacinės infrastruktūros saugą).

[1] Sąvokos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, 2014-12-11 Nr. XII-1428, 2 str., Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, 2011-12-15 Nr. XI-1807, 2 str. ir Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintame Bendrųjų elektroninės informacijos saugos reikalavimų apraše, 4 p.

[2] ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity.

[3] NATO Cooperative Cyber Defence Centre of Excellence National Cyber Security Framework Manual 2012 m.

Santrumpos:

CERT – Elektroninių ryšių tinklų ir informacijos saugumo tyrimo padalinys.

ES – Europos Sąjunga.

IRD – Informatikos ir ryšių departamentas prie Vidaus reikalų ministerijos.

IVPK – Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos.

KAM – Krašto apsaugos ministerija.

KSĮ – Kibernetinio saugumo įstatymas.

KS taryba – Kibernetinio saugumo taryba.

LRS – Lietuvos Respublikos Seimas.

LRV – Lietuvos Respublikos Vyriausybė.

NATO – Šiaurės Atlanto Sutarties Organizacija.

NKSC – Nacionalinis kibernetinio saugumo centras.

PAGD – Priešgaisrinės apsaugos ir gelbėjimo departamentas prie Vidaus reikalų ministerijos.

PD – Policijos departamentas prie Vidaus reikalų ministerijos.

RRT – Ryšių reguliavimo tarnyba.

SM – Susisiekimo ministerija.

SVDPT – Saugus valstybinis duomenų perdavimo tinklas.

VDAI – Valstybinė duomenų apsaugos inspekcija.

VIIV taryba – Valstybės informacinių išteklių valdymo taryba.

VRM – Vidaus reikalų ministerija.

SANTRAUKA

Lietuvos Respublikos Vyriausybė 2006 m. nustatė[4], kad galiojantis el. informacijos saugos (kibernetinio saugumo) srities reglamentavimas nepakankamas, todėl nutarė parengti el. ryšių tinklų ir informacijos saugumo įstatymą, o 2011 m. patvirtinto El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programą[5]. Tačiau ji vykdoma nerezultatyviai, o minėtas įstatymas taip ir nebuvo priimtas.

Taigi kibernetinio saugumo sritis iki 2015 m. rėmėsi teisės aktais, kuriuose nebuvo aiškiai nustatytų šios srities politiką formuojančių ir įgyvendinančių institucijų, kibernetinio saugumo dalyvių pareigų, atsakomybės, organizacinių ir techninių kibernetinio saugumo reikalavimų ir kibernetinio saugumo užtikrinimo priemonių.

2014 m. pabaigoje įvyko esminiai kibernetinio saugumo reglamentavimo pokyčiai: priimtas Kibernetinio saugumo įstatymas[6], nustatantis kibernetinio saugumo sistemos organizavimą, valdymą ir kontrolę, apibrėžiantis kibernetinio saugumo ir kitas pagrindines šios srities sąvokas. Įsigaliojus įstatymui (nuo 2015 m.), Krašto apsaugos ministerijai suteikti įgaliojimai formuoti kibernetinio saugumo politiką, organizuoti, kontroliuoti ir koordinuoti jos įgyvendinimą, Kibernetinio saugumo ir telekomunikacijų tarnyboje prie Krašto apsaugos ministerijos įsteigtas Nacionalinis kibernetinio saugumo centras[7], sudaryta Kibernetinio saugumo taryba[8].

Vidaus reikalų ministerija, iki 2015 m. turėjusi įgaliojimus formuoti valstybės politiką el. informacijos saugos, kibernetinio saugumo srityje, organizuoti, koordinuoti ir kontroliuoti jos įgyvendinimą[9], nuo 2015 m. politiką valstybės informacinių išteklių saugos srityje įgaliota formuoti tiek, kiek tai neapima kibernetinio saugumo[10] ir kartu su Nacionaliniu kibernetinio saugumo centru, Ryšių reguliavimo tarnyba, Valstybine duomenų apsaugos inspekcija ir Policijos departamentu pagal kompetenciją įgyvendinti kibernetinio saugumo politiką[11].

Kibernetinis saugumas Lietuvoje neatsiejamas nuo ES Kibernetinio saugumo strategijos, Komisijos direktyvos pasiūlymo dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti[12] ir susijęs su ES strategijos „Europa 2020“ dalimi

[4] Lietuvos Respublikos Vyriausybės 2006-12-06 nutarimu Nr. 1211 patvirtinta Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcija.

[5] Lietuvos Respublikos Vyriausybės 2011-06-29 nutarimu Nr. 796 patvirtinta Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa.

[6] Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014-12-11 Nr. XII-1428.

[7] Lietuvos Respublikos krašto apsaugos ministro 2014-12-29 įsakymu Nr. V-1321 patvirtinti Kibernetinio saugumo ir telekomunikacijų tarnybos prie Krašto apsaugos ministerijos nuostatai.

[8] Lietuvos Respublikos Vyriausybės 2015-04-23 nutarimu Nr. 422 patvirtinta Kibernetinio saugumo taryba ir jos reglamentas.

[9] Lietuvos Respublikos Vyriausybės 2001-03-14 nutarimu Nr. 291 patvirtinti Lietuvos Respublikos vidaus reikalų ministerijos nuostatai 8.6. p.

[10] Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807 (akto redakcija, galiojanti nuo 2015-01-01 su paskutiniu pakeitimu, atliktu 2014-11-06 įstatymu Nr. XII-1302), 5 str. 4 d.

[11] Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014-12-11 Nr. XII-1428, 4 str. 2 ir 3 d.

[12] Europos Sąjungos vyriausiojo įgaliotinio užsienio reikalams 2013-02-07 bendras komunikatas JOIN (2013) 1 final Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Europos Sąjungos kibernetinio saugumo strategija“ kartu su Europos Komisijos pasiūlymu dėl Europos Parlamento ir Tarybos direktyvos dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti COM(2013) 48 final.

„Europos skaitmeninė darbotvarkė“ [13], kurioje pabrėžiama, jog visos suinteresuotosios šalys turi kartu stengtis užtikrinti informacinių ir ryšių technologijų infrastruktūros saugumą ir atsparumą, daugiausia dėmesio skiriant prevencijai, parengčiai ir informuotumui, kad būtų sukurti veiksmingi ir suderinti reagavimo į naujas ir vis sudėtingesnes kibernetines atakas ir el. nusikaltimus mechanizmai.

Valstybės mastu nėra sukaupta tikslių duomenų apie kibernetinio saugumo ir el. informacijos saugos priemonėms įgyvendinti naudojamas lėšas. Valstybinių auditorių vertinimu, 2011–2014 m. kibernetinio saugumo ir el. informacijos saugos priemonėms įgyvendinti panaudota apie 20,9 mln. EUR, o nuo 2015 m. iki 2020 m. planuojama panaudoti dar apie 15,6 mln. EUR valstybės biudžeto asignavimų, ES ir kitos tarptautinės finansinės paramos lėšų.

Audito tikslas – įvertinti, ar užtikrinamas kibernetinis saugumas Lietuvoje. Tikslui pasiekti vertinome, ar:

- sukurta veiksminga kibernetinio saugumo sistema;
- užtikrinamas kibernetinis saugumas valstybinėse įstaigose.

Audito metu analizavome esamą kibernetinio saugumo ir el. informacijos saugos teisinį reguliavimą, strateginį planavimą, valdymo praktiką, šiai sričiai skiriamas ir naudojamas lėšas. Vertinome, ar pasiekti planavimo dokumentuose nustatyti kibernetinio saugumo ir el. informacijos saugos rezultatai ir kaip valstybės įstaigos užtikrina kibernetinį saugumą, ar tinkamai taiko kibernetinio saugumo technines ir organizacines priemones.

Auditą atlikome Vidaus reikalų ministerijoje ir Krašto apsaugos ministerijoje. Duomenis ir informaciją rinkome iš šių ministerijų valdymo srities įstaigų, kitų ministerijų, Vyriausybės kanceliarijos, Ryšių reguliavimo tarnybos, Valstybinės duomenų apsaugos inspekcijos, Valstybės saugumo departamento, Lietuvos mokslo ir studijų institucijų kompiuterinio tinklo (LITNET) tarybos atstovų ir Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos. Bendravome su asociacijos „INFOBALT“ kibernetinio saugumo specialistais. Audito metu aštuoniolikoje įstaigų atlikome patikras vietoje. Analizavome užsienio šalių patirtį, gerąją praktiką, mokslinių tyrimų duomenis ir visuomenės informavimo priemonėse skelbiamą informaciją, susijusią su audituojama sritimi.

Audituojamas laikotarpis – 2011–2015 m. I pusmetis. Pokyčių analizei buvo naudojami ankstesnių laikotarpių duomenys.

Nustatėme, kad iki šiol valstybėje nepakankamai efektyviai sprendžiami kibernetinio saugumo ir jo atsparumo didinimo klausimai. Akcentuojant tik reagavimą į incidentus ir jų užkardymą kibernetinėje erdvėje, pamirštami tradiciniai el. informacijos saugos valdymo klausimai (informacijos konfidencialumas, vientisumas, prieinamumas) ir nuo 2015 m. neskiriama pakankamai dėmesio šios srities plėtrai, teisės aktų rengimui, organizacinės struktūros tobulinimui ir kt.

Be to, viešajame sektoriuje įgyvendinamos nepakankamos šios srities organizacinės ir techninės priemonės. Valstybinės įstaigos savo veikloje nepakankamai dėmesio skiria kibernetiniam saugumui užtikrinti, o naujai priimtas Kibernetinio saugumo įstatymas neišsprendžia visų su kibernetiniu saugumu susijusių grėsmių. Šis įstatymas bus veiksmingas tiek, kiek bus veiksmingi jį lydintieji teisės aktai, įstaigų praktinė patirtis ir gebėjimai valdyti kibernetinį saugumą ir el. informacijos saugą, parinkti efektyvias reikalavimų įgyvendinimo kontrolės priemones, spręsti

[13] Europos Komisijos 2010-08-26 komunikato KOM(2010) 245 galutinis/2 Europos Parlamentui, Tarybai, Europos Ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Europos Skaitmeninė darbotvarkė“ 2.3 dalis.

šios srities specialistų kompetencijos problemas. Nepašalinus šių trūkumų gali nukentėti ne tik administracinės ir viešosios paslaugos, informacija, bet ir kiekvienas pilietis, šalies prestižas, pasitikėjimas naujomis technologijomis.

Siekiant tobulinti kibernetinio saugumo reglamentavimo kokybę, spręsti esamas planavimo ir finansavimo problemas, pasiūlėme Vyriausybei nustatyti bendras kibernetinio saugumo, el. informacijos saugos strategines kryptis ir joms pasiekti būtinas priemones, konsoliduoti el. informacijos saugos valdymą. Skirti įstaigą, kuri koordinuotų šios srities reikalavimų rengimą, jų suvienijimą ir nustatyti lėšų skyrimo, panaudojimo prioritetus ir kriterijus.

Krašto apsaugos ir Vidaus reikalų ministerijoms rekomendavome peržiūrėti esamus kibernetinio saugumo, el. informacijos saugos reikalavimus, juos suderinti, patvirtinti šios srities trūkstamas nuostatas, metodinius dokumentus ir numatyti priemones, skirtas konsultuoti ir informuoti kibernetinį saugumą, el. informacijos saugą užtikrinančius subjektus aktualiais šios srities klausimais.

Įvertinę audito metu surinktus įrodymus, pateikiame valstybinio audito išvadas ir rekomendacijas.

IŠVADOS

1. Kibernetinio saugumo ir el. informacijos saugos sritys Lietuvoje atskirtos įstatymų lygiu, tačiau juos įgyvendinti nėra lengva, o bendra valstybės saugumo būklė šiose srityse kol kas negerėja, nes:

   1.1. El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programa, kurioje planuota pasiekti daugiausia rezultatų šioje srityje, vykdoma nerezultatyviai (bendras programos tikslų įgyvendinimas 2015 m. rugsėjo mėn. siekia 21 proc.). Nustatyti ne visi su kibernetinio saugumo ir el. informacijos sauga susijusių planavimo dokumentų tarpusavio ryšiai, vėluojama įgyvendinti planavimo dokumentuose numatytas priemones (1.1 poskyris, 11–14 psl.);

   1.2. laiku neparengti teisės aktai, reglamentuojantys kibernetinį saugumą, nėra sprendimo dėl el. informacijos saugos, kibernetinio saugumo ir kitų su informacijos sauga susijusių sričių reikalavimų peržiūrėjimo ir suderinimo (1.2 poskyris, 15–17 psl.);

   1.3. 2015 m. pradėjusi veikti kibernetinio saugumo valdymo sistema nesudaro visų su el. informacijos sauga susijusių sričių darnaus valdymo sąlygų: neišvengiama dalinio įstaigų veiklos dubliavimo, trūksta kompetencijos atskyrimo formuojant ir įgyvendinant kibernetinio saugumo ir el. informacijos saugos politiką (1.3 poskyris, 18–19 psl.);

   1.4. kibernetiniam saugumui ir el. informacijos saugai reikalingų lėšų skyrimas ir panaudojimas (suplanuota 2015–2020 m. 15,6 mln. EUR) vykdomas šių sričių politiką formuojančioms Krašto apsaugos ir Vidaus reikalų ministerijoms nenustačius lėšų skyrimo prioritetų ir kriterijų, neturint duomenų apie faktinę įstaigų kibernetinio saugumo ir el. informacijos saugos būklę, panaudotas lėšas (2011–2014 m. 20,9 mln. EUR) ir jų poveikį (1.4 poskyris, 19–22 psl.).

2. Kibernetinio saugumo ir el. informacijos saugos techninių ir organizacinių priemonių įgyvendinimas viešajame sektoriuje nepakankamas, netinkamai pasiruošta reaguoti į kibernetinėje erdvėje kylančias grėsmes, nes tikrintos įstaigos:

   2.1. vidutiniškai taiko 25 proc. šiai sričiai užtikrinti rekomenduojamų organizacinių priemonių, pagrindiniai trūkumai susiję su saugumo valdymo sistemos kūrimu, incidentų valdymu, veiklos tęstinumo užtikrinimu, personalo kompetencijos tobulinimu ir išoriniu bendradarbiavimu;

   2.2. tinkamai įgyvendina tik 39 proc. rekomenduojamų techninių priemonių ir lieka pažeidžiamos dėl netinkamo saugios konfigūracijos nustatymo, el. ryšių tinklų, mobilių ir kitų technologijų valdymo (2 skyrius, 23–26 psl.).

REKOMENDACIJOS

Lietuvos Respublikos Vyriausybei:

1. Siekiant užtikrinti kibernetinį saugumą ir jo atsparumo didinimą, tobulinti esamą planavimą, teisinį reguliavimą ir finansų valdymą:

   1.1. nustatyti bendras kibernetinio saugumo, el. informacijos saugos strategines kryptis ir joms pasiekti būtinas priemones (1.1 išvada);

   1.2. skirti įstaigą, kuri valstybės mastu koordinuotų kibernetinio saugumo, el. informacijos saugos reikalavimų rengimą, jų suvienijimą (1.2 išvada);

   1.3. konsoliduoti el. informacijos saugos valdymą (1.3 ir 2 išvados);

   1.4. valstybės mastu nustatyti kibernetiniam saugumui, el. informacijos saugai reikalingų lėšų skyrimo ir panaudojimo prioritetus, kriterijus, stebėsenos ir kontrolės mechanizmą (1.4 išvada).

Lietuvos Respublikos krašto apsaugos ir vidaus reikalų ministerijoms:

2. Siekiant gerinti kibernetinio saugumo reglamentavimo kokybę ir efektyvumą, mažinti administracinę naštą šiuos reikalavimus įgyvendinančioms ir jų įgyvendinimą stebinčioms įstaigoms:

   2.1. peržiūrėti esamus kibernetinio saugumo, el. informacijos saugos reikalavimus, juos suderinti ir (arba) patvirtinti trūkstamas nuostatas ir metodinius dokumentus (1.2 ir 2 išvados);

   2.2. užtikrinti įstaigų konsultavimą ir informavimą kibernetinio saugumo ir el. informacijos saugos (valdymo sistemos kūrimas, incidentų valdymas, veiklos tęstinumo užtikrinimas, personalo kompetencijos tobulinimas, išorinis bendradarbiavimas, saugios konfigūracijos nustatymas, tinklo saugumas, mobilių ir kitų technologijų valdymas) klausimais (2 išvada).

Rekomendacijų įgyvendinimo priemonės ir terminai pateikti 1 priede.

ĮŽANGA

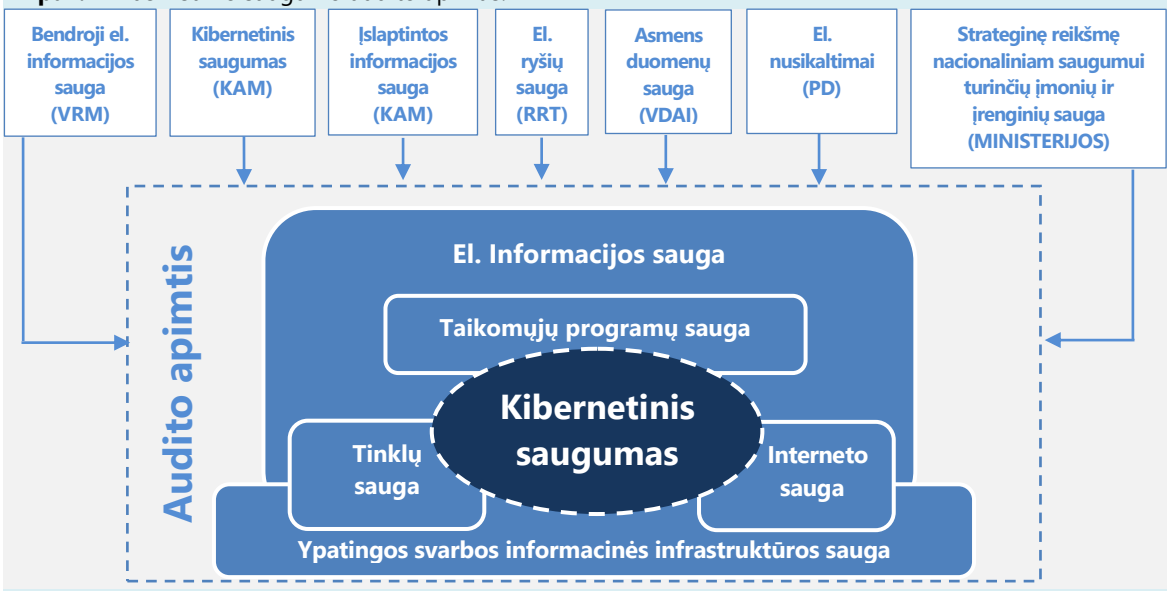
Kibernetinio saugumo įstatymas[14] apibrėžia, kad kibernetinis saugumas – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei el. ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti.

Iki Kibernetinio saugumo įstatymo įsigaliojimo (2015 m.) ši sąvoka teisės aktuose nebuvo apibrėžta, o kibernetinis saugumas buvo suvokiamas kaip el. informacijos saugos sudėtinė dalis, kibernetiniam saugumui užtikrinti buvo numatytos ir taikomos el. informacijos kontrolės priemonės, įskaitant kibernetinių incidentų stebėsenos priemones.

Įsigaliojus Kibernetinio saugumo įstatymui el. informacijos saugos ir kibernetinio saugumo sričių reglamentavimas formaliai buvo atskirtas, o el. informacijos sauga buvo reglamentuojama Valstybės informacinių išteklių valdymo įstatymo ir kitų teisės aktų nuostatomis[15]. Nepaisant teisinio atskyrimo, taikomos organizacinės ir techninės priemonės (atliekant rizikos vertinimus, nustatant saugos valdymo sistemą, parenkant kontrolės priemones ir kt.), yra tarpusavyje susijusios ir papildo viena kitą.

Atsižvelgiant į tarptautinių standartų ir metodikų pateikiamus kibernetinio saugumo apibrėžimus ir valdymo praktiką, kibernetinis saugumas šioje audito ataskaitoje nagrinėtas plačiau, kartu su kitomis saugos sritimis (žr. 1 pav.). Pagal Tarptautinės standartizacijos organizacijos standartuose ir Šiaurės Atlanto Sutarties Organizacijos Kibernetinės gynybos tobulinimo kompetencijos centro rekomendacijas kibernetinis saugumas tiesiogiai susijęs su el. informacijos, taikomųjų programų, tinklų, interneto ir ypatingos svarbos informacinės infrastruktūros saugos sritimis.

1 pav. Kibernetinio saugumo audito apimtis.



Šaltinis – Valstybės kontrolė pagal ISO standarto[16] ir NATO Kibernetinės gynybos tobulinimo kompetencijos centro pateiktas rekomendacijas[17].

[14] Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014-12-11 Nr. XII-1428, 2 str. 5 d.

[15] El. informacijos, kurios turinį sudaro asmens duomenys, tvarkymo saugumas užtikrinamas vadovaujantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu; el. informacijos (duomenų), generuojamos (-ų) arba tvarkomos (-ų) teikiant viešąsias el. ryšių paslaugas, tvarkymo ir privatumo apsauga užtikrinama vadovaujantis Lietuvos Respublikos elektroninių ryšių įstatymu; el. informacijos, kuri įslaptinta, automatizuoto apdorojimo ir perdavimo apsauga užtikrinama vadovaujantis Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymu ir kt.

[16] ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity.

El. informacijos saugos ir kibernetinio saugumo plėtrai užtikrinti Lietuvos Respublikos Vyriausybė 2006 m. patvirtino El. ryšių tinklų ir informacijos saugumo įstatymo koncepciją[18], 2011 m. – tarpinstitucinę plėtros programą[19]. 2012 m. Nacionalinio saugumo strategijoje[20] kibernetinio saugumo ir informacijos saugos sritys įvardytos tarp pirmaeilių nacionalinio saugumo interesų, o nuo 2015 m. kibernetinio saugumo stiprinimas įvardytas kaip vienas iš Vyriausybės veiklos prioritetų[21].

Pastaruosius keletą metų ilgos ir vidutinės trukmės valstybės planavimo dokumentuose deklaruojama parama el. informacijos saugos, kibernetinio saugumo plėtrai, nuo 2015 m. įsigaliojo Kibernetinio saugumo įstatymas, tačiau to nepakako, kad valstybė sistemiškai sureguliuotų strategiškai svarbias kibernetinio saugumo ir el. informacijos saugos sritis. Vis dar atsiliekame nuo planuotų terminų, trūksta koordinavimo, kompleksinio požiūrio valdant kibernetinio saugumo ir el. informacijos saugos sritis. Kasmet užregistruojama vis daugiau pranešimų apie incidentus kibernetinėje erdvėje (Ryšių reguliavimo tarnybos duomenimis[22] 2014 m. saugumo incidentų skaičius, lyginant su ankstesniais metais, išaugo 43 proc.). Žvalgybos institucijų 2015 m. duomenimis[23] kibernetinių incidentų skaičius bent jau artimiausiu metu nemažės, pati kibernetinė erdvė liks viena pagrindinių veiklos erdvių vykdant ir šnipinėjimą, ir kitaip veikiant svarbius Lietuvos nacionaliniam saugumui ir šalies gynybinei galiai kritinės infrastruktūros objektus.

Auditas atliktas pagal Valstybinio audito reikalavimus[24] ir Tarptautinius aukščiausiųjų audito institucijų standartus[25]. Atlikdami auditą darėme prielaidą, kad visi auditoriams pateikti dokumentai yra teisingi, išsamūs ir galutiniai, o jų kopijos atitinka originalus. Informacija apie audito duomenų rinkimo ir vertinimo metodus pateikta 2 priede.

[17] NATO Cooperative Cyber Defence Centre of Excellence National Cyber Security Framework Manual 2012 m.

[18] Lietuvos Respublikos Vyriausybės 2006-12-06 nutarimu Nr. 1211 patvirtinta Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcija.

[19] Lietuvos Respublikos Vyriausybės 2011-06-29 nutarimu Nr. 796 patvirtinta Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa.

[20] Lietuvos Respublikos Seimo 2012-05-28 nutarimu Nr. IX-907 patvirtintos Nacionalinio saugumo strategijos 8.7 ir 8.8 p.

[21] Lietuvos Respublikos Vyriausybės 2014-10-03 nutarimu Nr. 1094 patvirtintų Lietuvos Respublikos Vyriausybės 2015 m. veiklos prioritetų 5.3 p.

[22] Ryšių reguliavimo tarnybos Nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio 2014 m. veiklos ataskaita https://www.cert.lt/statistika.html.

[23] Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos 2015 m. parengto Grėsmių nacionaliniam saugumui vertinimas, 22 psl.

[24] Patvirtinta Lietuvos Respublikos valstybės kontrolieriaus 2002-02-21 įsakymu Nr. V-26 (2012-06-28 Nr. V-171 redakcija).

[25] 3000-asis TAAIS „Veiklos audito įgyvendinimo gairės“ ir 3100-asis TAAIS „Veiklos audito gairės: pagrindiniai principai“ (http://www.vkontrole.lt/page.aspx?id=350).

AUDITO REZULTATAI

1. NESUKURTA VEIKSMINGA KIBERNETINIO SAUGUMO SISTEMA

Kibernetinio saugumo įstatymas [26] nustato kibernetinio saugumo sistemos organizavimą, valdymą ir kontrolę, tačiau neapibrėžia kibernetinio saugumo sistemos sąvokos ir apsiriboja įvairių teisinių, informacijos sklaidos, organizacinių ir techninių priemonių nustatymu kibernetiniam saugumui užtikrinti.

Vertindami kibernetinį saugumą nagrinėjome keturias sritis (žr. 2 pav.), kurių sėkmingas valdymas turėtų padėti valstybės institucijoms, įstaigoms ir kitiems suinteresuotiems subjektams užtikrinti geresnės kokybės kibernetinio saugumo organizavimą, valdymą ir kontrolę.

2 pav. Audito metu nagrinėtos sritys.

Šaltinis – Valstybės kontrolė.

Laikėmės nuostatos, kad kibernetinio saugumo sistema veiksminga, kai:

- pasiekiami planuoti rezultatai, racionaliai valdomi finansai (nustatyti lėšų skyrimo prioritetai ir kriterijai; skaičiuojamas planuotų ir panaudotų lėšų kiekis; vertinamas skiriamų lėšų suderinamumas su kibernetinio saugumo politika);
- nustatyti visi taikytini reikalavimai ir ypatingos svarbos informacinės infrastruktūros objektai;
- užtikrinamas darnus kibernetinio saugumo ir el. informacijos saugos valdymas (nustatytos politikos formavimo ir įgyvendinimo atsakomybės, jos nepersidengia, nesidubliuoja ir yra vykdomos).

1.1. Nepasiekti planuoti kibernetinio saugumo ir el. informacijos saugos rezultatai

Išnagrinėję audito metu galiojusius valstybės planavimo dokumentus, nustatėme, kad kibernetinio saugumo ir el. informacijos saugos rezultatai nustatyti įvairios trukmės planavimo dokumentuose (3 pav.), tačiau daugiausia rezultatų šiose srityse planuojama pasiekti įgyvendinant El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programą[27]. Tai Vidaus reikalų ministerijos koordinuojama tarpinstitucinė programa, kurioje nustatyti 3 įgyvendinimo tikslai, 10 uždavinių, 59 vertinimo kriterijai ir siekiamos jų reikšmės 2011, 2015 ir 2019 m. (už kriterijų įgyvendinimą atsakingos trylika institucijų ir įstaigų, taip pat viešojo administravimo institucijos, teikiančios paslaugas kibernetinėje erdvėje[28]).

[26] Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014-12-11 Nr. XII-1428, 1 str. 1 d.

[27] Lietuvos Respublikos Vyriausybės 2011-06-29 nutarimu Nr. 796 patvirtinta Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa.

[28] Ten pat, programos priedo 59 p.

Nustatėme, kad penkerius metus vykdoma El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programa nerezultatyvi: 2015 m. rugsėjo mėn. pasiekta tik 23 proc. planuotų rodiklių, 48 proc. pasiekti iš dalies, 29 proc. – nepasiekta. Esama būklė rodo, kad 2015 m. nebus pasiektas nė vienas programoje numatytas tikslų rodiklis, o bendras programos tikslų įgyvendinimas kol kas siekia tik 21 proc. (žr. 1 lentelę).

1 lentelė. El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programos rezultatai (2015 m. rugsėjo mėn. duomenys).

Tikslai ir jų vertinimo kriterijai	Rodikliai			Uždaviniai	Rodikliai**		
	P	D	F*		+	+/-	-
Pasiekti, kad būtų užtikrintas valstybės informacinių išteklių saugumas.							
Saugos reikalavimus atitinkančių valstybės informacinių išteklių dalis procentais.	**95%**	**75%**	**24%**	Tobulinti eKS koordinavimą ir priežiūrą.	17%	42%	41%
				Tobulinti eKS teisinį reglamentavimą.	20%	40%	40%
				Plėsti ir tobulinti saugią valstybės informacinę infrastruktūrą.	0%	80%	20%
				Skatinti eKS projektų įgyvendinimą.	0%	100%	0%
				Plėtoti tarptautinį bendradarbiavimą eKS srityje.	83%	17%	0%
Užtikrinti veiksmingą ypatingos svarbos informacinės infrastruktūros funkcionavimą.							
Vidutinis ypatingos svarbos informacinės infrastruktūros objektų incidentų likvidavimo laikas valandomis.	**1 val. (100%)**	**12 val. (8%)**	**17%**	Užtikrinti ypatingos svarbos informacinės infrastruktūros saugumą.	17%	8%	75%
Užtikrinti Lietuvos gyventojų ir asmenų, esančių Lietuvoje, saugumą kibernetinėje erdvėje.							
Lietuvos gyventojų, kurie saugiai jaučiasi kibernetinėje erdvėje, dalis procentais.	**40%**	**Nematuota**	**23%**	Kelti eKS kultūrą.	40%	50%	10%
				Stiprinti Lietuvos kibernetinės erdvės saugumą.	50%	25%	25%
				Užtikrinti virtualaus Lietuvos kibernetinės erdvės perimetro apsaugą nuo išorinių kibernetinių atakų.	0%	50%	50%
				Stiprinti kibernetinėje erdvėje teikiamų paslaugų saugumą.	0%	67%	33%
VISO:			**21%**	**VISO*:**	**23%**	**48%**	**29%**
P – 2015 m. planuota pasiekti reikšmė. D – Vidaus reikalų ministerijos duomenys.			F, * – faktinis uždavinių pasiekto lygio vidurkis pagal Valstybės kontrolės surinktus duomenis. eKS – el. informacijos sauga (kibernetinis saugumas). ** – pagal programoje numatytus vertinimo kriterijus.		Pasiekta / Iš dalies/ Nepasiekta		

Šaltinis – Valstybės kontrolė pagal Vidaus reikalų ministerijos ir programą įgyvendinančių įstaigų duomenis.

Išanalizavę, kaip koordinuojama ir įgyvendinama El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programa, nustatėme, kad neefektyvus programos koordinavimas ir ją įgyvendinančių įstaigų nepakankamas aktyvumas atsirado dėl šių pagrindinių priežasčių:

- uždavinių, institucijų ir įstaigų gausiai programai Vidaus reikalų ministerija nerengė tarpinstitucinio veiklos plano (padeda koordinatoriui veiksmingai įgyvendinti tikslus ir uždavinius, nustato asignavimų poreikį) arba veiksmų plano (detalūs veiksmai ir reikiamų asignavimų skyrimas, kurį galima pasiekti tarpinstituciniu susitarimu), o nustatytiems vertinimo kriterijams aprašyti – techninių priedų (paaiškinimų, kas vertinama ir kaip), kaip tai nurodo Strateginio planavimo metodika[29];
- prižiūrėdama, kaip įgyvendinami programos tikslai, uždaviniai, atlikdama tarpinę joje numatytų uždavinių, vertinimo kriterijų reikšmių ir jų pokyčių peržiūrą, Vidaus reikalų ministerija nenumatė, kaip bus matuojamas programos uždavinių pasiekimas ir programos poveikis; neužtikrino tinkamo programos dalyvių atsiskaitymo už siekiamus rezultatus, neinicijavo programos nuostatų atnaujinimo, nors jos įgyvendinime dalyvaujančios įstaigos teikė siūlymus programos tobulinimui, 2012–2015 m. keitėsi šios srities reguliavimas, o 2014 m. ES institucijos paskelbė programos rengimo trūkumus ir tobulinimo galimybes[30];

[29] Lietuvos Respublikos Vyriausybės 2002-06-06 nutarimu Nr. 827 patvirtintos Strateginio planavimo metodikos 13, 22^1, 22^2, 44 p.

[30] Europos tinklų ir informacijos saugumo agentūros 2014 m. ataskaita „An evaluation framework for cyber security strategies".

- tik kai kurios programos įgyvendinime dalyvaujančios įstaigos (pvz.: Krašto apsaugos ministerija) atsižvelgdamos į joje numatytus uždavinius ir siekiamus rezultatus, savo strateginiuose ir (arba) metiniuose veiklos planuose numatė rezultato pasiekimo reikšmes planuojamu laikotarpiu, pasirinko atitinkamas priemones ir planavo lėšas, kaip tai buvo numatyta programoje.

Taigi Vidaus reikalų ministerija ir kitos[31] už El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programos kriterijų įgyvendinimą atsakingos įstaigos negalėjo tinkamai pasiruošti programoje numatytų uždavinių įgyvendinimui, susiderinti asignavimus ir užtikrinti, kad pasiekti rezultatai atitiktų joje keliamus tikslus. Vidaus reikalų ministerija laiku negavo šios programos koordinavimui reikiamos informacijos, neturi tikslių duomenų apie programos įgyvendinimo eigą (vertinimo kriterijų reikšmių nepasiekimo ar viršijimo priežastis, įgyvendinimo rizikas, programos vykdymui panaudotas lėšas, tikslų dalyvių skaičių ir kt.), todėl Seimo komitetams, Vyriausybei ir visuomenei teikiama nepakankamai tiksli informacija apie programos koordinavimą ir įgyvendinimą. Pažymėtina, kad šios programos nuostatos, planuotų uždavinių vykdytojai ir turinys jau keletą metų neatitinka pasikeitusio šios srities reglamentavimo, todėl praranda aktualumą ir turėtų būti peržiūrėtos.

Krašto apsaugos ministerijos nuomonė[32]

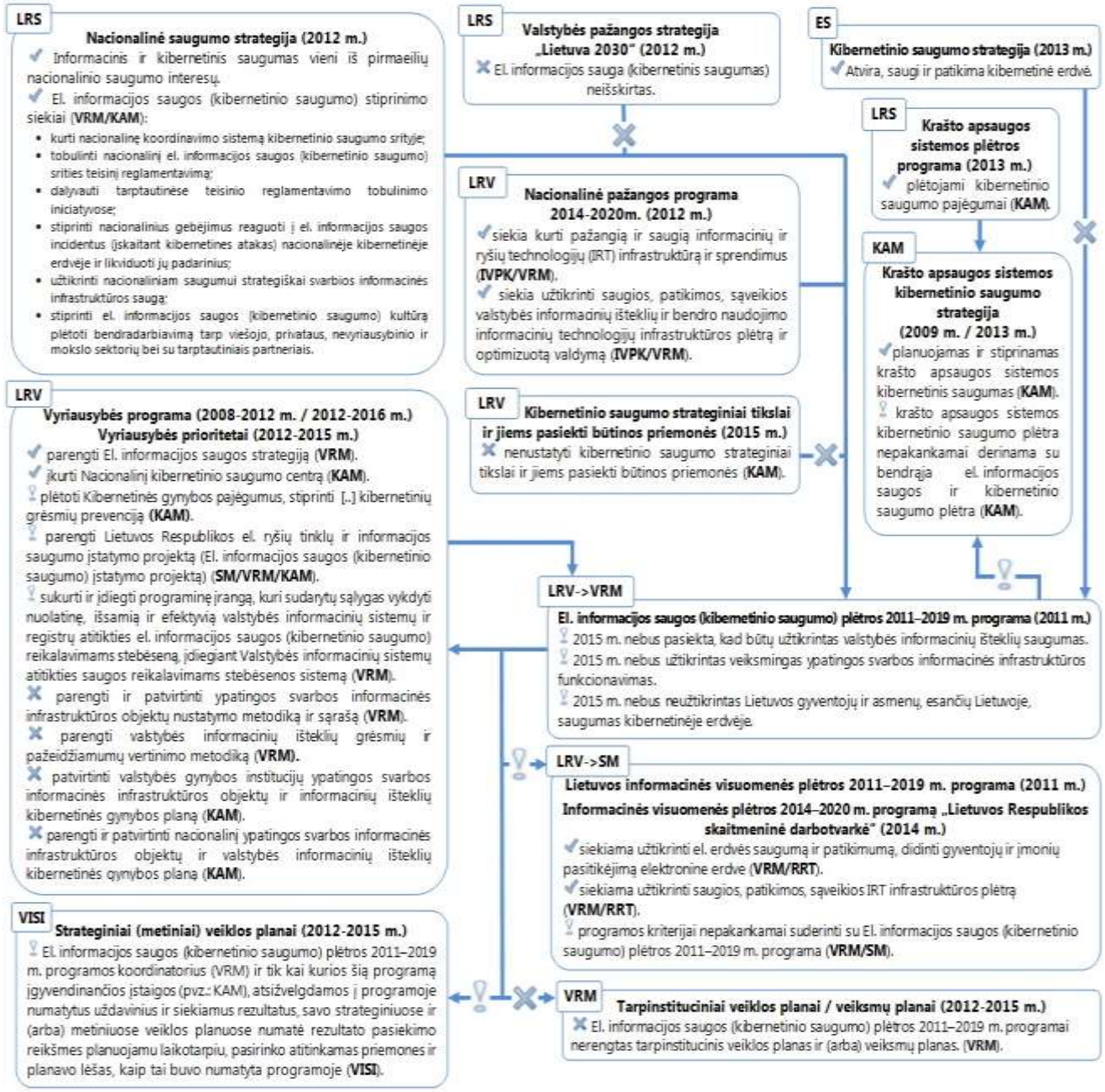
> Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programoje, patvirtintoje Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimu Nr. 796 „Dėl Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programos patvirtinimo“ (toliau – Programa), nustatyti jos įgyvendinimo vertinimo kriterijai ir siekiamos jų reikšmės 2015 m., kurių atžvilgiu galėtų būti įvertinta kibernetinio saugumo būklės pokyčiai nuo programos įgyvendinimo pradžios (2011 – 2015 m. laikotarpis). Atkreiptinas dėmesys, kad vadovaujantis Programos 14.2 papunkčiu, informacija apie Programos įgyvendinimą 2015 m. Vidaus reikalų ministerijai turėtų būti pateikta iki 2016 m. vasario 1 d. Alternatyviai galėtų būti įvertinta kibernetinio saugumo būklė iki įsigaliojant KSĮ. Audituojamas laikotarpis (2011 m. – 2015 m. I pusmetis) mūsų nuomone nekoreliuoja nei su Programos, nei su KSĮ įsigaliojimo terminais.

Nagrinėjant kitus ilgos, vidutinės trukmės ir trumpalaikius planavimo dokumentus pastebėjome, kad ne visi su kibernetiniu saugumu ir el. informacijos sauga susiję planavimo dokumentai dera tarpusavyje, vėluojama įgyvendinti priemones arba jos neįgyvendinamos, todėl kibernetinio saugumo ir el. informacijos saugos plėtra nevientisa, trūksta kompleksinio požiūrio į šių sričių plėtros planavimą (žr. 3 pav.).

[31] Lietuvos Respublikos Vyriausybės 2011-06-29 nutarimu Nr. 796 patvirtintos Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos tikslus ir uždavinius įgyvendina: Vidaus reikalų ministerija, Krašto apsaugos ministerija, Susisiekimo ministerija, Valstybinė duomenų apsaugos inspekcija, Ryšių reguliavimo tarnyba, Policijos departamentas prie Vidaus reikalų ministerijos, Vyriausybės kanceliarija, Lietuvos mokslo ir studijų institucijų kompiuterinio tinklo LITNET taryba, Švietimo ir mokslo ministerija, Valstybės saugumo departamentas, Ūkio ministerija, Energetikos ministerija, Finansų ministerija ir viešojo administravimo institucijos, teikiančios paslaugas kibernetinėje erdvėje.

[32] Lietuvos Respublikos krašto apsaugos ministerijos 2015-12-09 raštas Nr. 12-01-2369.

3 pav. El. informacijos sauga ir kibernetinis saugumas planavimo dokumentuose.



✓ atlikta ? vėluota atlikti ir (arba) nustatyta suderinamumo trūkumų ✗ neatlikta ir (arba) nesuderinta tarpusavyje

Šaltinis – Valstybės kontrolė.

Kibernetinio saugumo plėtra gali padėti pagrindus atsirasti naujos kokybės el. informacijos saugos planavimo dokumentams, tačiau valstybėje lieka tiek sena neperžiūrėta el. informacijos saugos planavimo visumą, tiek bandoma planuoti naują kibernetinio saugumo srities plėtrą, kurios kokybė priklausys nuo kompleksinio visų su šia sritimi susijusių planavimo dokumentų peržiūrėjimo ir suderinimo. Vyriausybė, Krašto apsaugos ir Vidaus reikalų ministerijos ir kiti kibernetinio saugumo dalyviai iki 2014 m. gruodžio 31 d. turėjo priimti Kibernetinio saugumo įstatymo įgyvendinamuosius teisės aktus[33], tačiau, praėjus beveik metams po įstatymo įsigaliojimo, dar neperžiūrėti esami ir nenustatyti nauji kibernetinio saugumo politikos strateginiai tikslai ir jiems pasiekti būtinos priemonės. Krašto apsaugos ministerija (pradėjusi formuoti valstybės kibernetinio saugumo politiką) ir Vidaus reikalų ministerija (formuojanti

[33] Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014-12-11 Nr. XII-1428, 20 str. 2 d.

valstybės el. informacijos saugos politiką, tiek, kiek tai neapima kibernetinio saugumo) dar nenusprendė dėl būsimų kibernetinio saugumo ir el. informacijos saugos plėtros krypčių ir siektinų rezultatų įgyvendinimo.

Kol nenustatyti nauji kibernetinio saugumo politikos strateginiai tikslai ir nesutarta dėl el. informacijos saugos plėtros krypčių ir siektinų rezultatų įgyvendinimo, tikslinga peržiūrėti El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programą. Reikėtų nustatyti ir kibernetinio saugumo, ir el. informacijos saugos bendrus tikslus, kurie užtikrintų šios srities darnią, nuoseklią ir kokybišką plėtrą.

Siekiant tobulinti kibernetinio saugumo ir el. informacijos saugos plėtros planavimą, Krašto apsaugos ministerijai kartu su Vidaus reikalų ministerija tikslinga peržiūrėti esamus planavimo dokumentus ir pateikti Vyriausybei siūlymus dėl bendros kibernetinio saugumo ir el. informacijos saugos plėtros krypčių ir siektinų rezultatų įgyvendinimo strategijos tvirtinimo. Tinkamas strategijos pasirinkimas ir darbų planavimas turėtų padėti šalinti po Kibernetinio saugumo įstatymo įsigaliojimo likusius kibernetinio saugumo ir el. informacijos saugos organizacinės struktūros, finansų valdymo ir kitus trūkumus.

1.2. Kibernetinio saugumo ir el. informacijos saugos reguliavimas turi trūkumų

Analizuodami teisės aktus, susijusius su kibernetiniu saugumu ir jų rengimo planus, nustatėme, kad teisės aktai reglamentuojantys kibernetinį saugumą nebuvo parengti laiku. Rengiant kibernetinio saugumo srities reikalavimus neplanuojama peržiūrėti visų iki šiol galiojančių su el. informacijos sauga susijusių reikalavimų, nėra sprendimo dėl el. informacijos saugos, kibernetinio saugumo ir kitų su informacijos sauga susijusių sričių reikalavimų suderinimo.

Įstatymo, reglamentuojančio kibernetinio saugumo sritį, priėmimo procedūros tęsėsi aštuonerius metus (priimtas 2014 m. gruodžio 11 d.), jį įgyvendinantys teisės aktai nepriimti iki įstatymo įsigaliojimo (2015 m.), kaip tai nustatė Kibernetinio saugumo įstatymas[34] ir vis dar rengiami iki šiol (parengta 43 proc., neparengta (ir vėluojama rengti) 57 proc.).

Pagrindinis trikdis, stabdantis šios srities reikalavimų rengimą – trejus metus (nuo 2012 m.) Vidaus reikalų ministerijos rengiamas ypatingos svarbos informacinės infrastruktūros (valdytojų) sąrašas, jos identifikavimo metodika.

Nustatėme ir kitų kibernetinio saugumo srities reglamentavimo trūkumų, kurie liko 2015 m. įsigaliojus Kibernetinio saugumo įstatymui ir kuriuos kaip svarbiausius audito metu įvardijo tikrintos įstaigos (žr. 4 pav.). Taigi kol kas šios srities teisinis reguliavimas nepakankamas, kad būtų galima veiksmingai užtikrinti valstybės kibernetinį saugumą.

[34] Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014-12-11 Nr. XII-1428, 20 str. 2 d.

4 pav. Kibernetinio saugumo srities reglamentavimo būklė (2015 m. rugsėjo mėn.).

	VISO 100% (23)	VRM 26% (6)	NKSC 9% (2)	KAM 30% (7)	LRV 13% (3)	Kiti* 22% (5)
Parengta	43% (10)	0% (0)	0% (0)	43% (3)	67% (2)	100% (5)
Rengiama	57% (13)	100% (6)	100% (2)	57% (4)	33% (1)	0% (0)

* – RRT, VDAI ir PD.

Parengta Rengiama ir (arba) peržiūrima

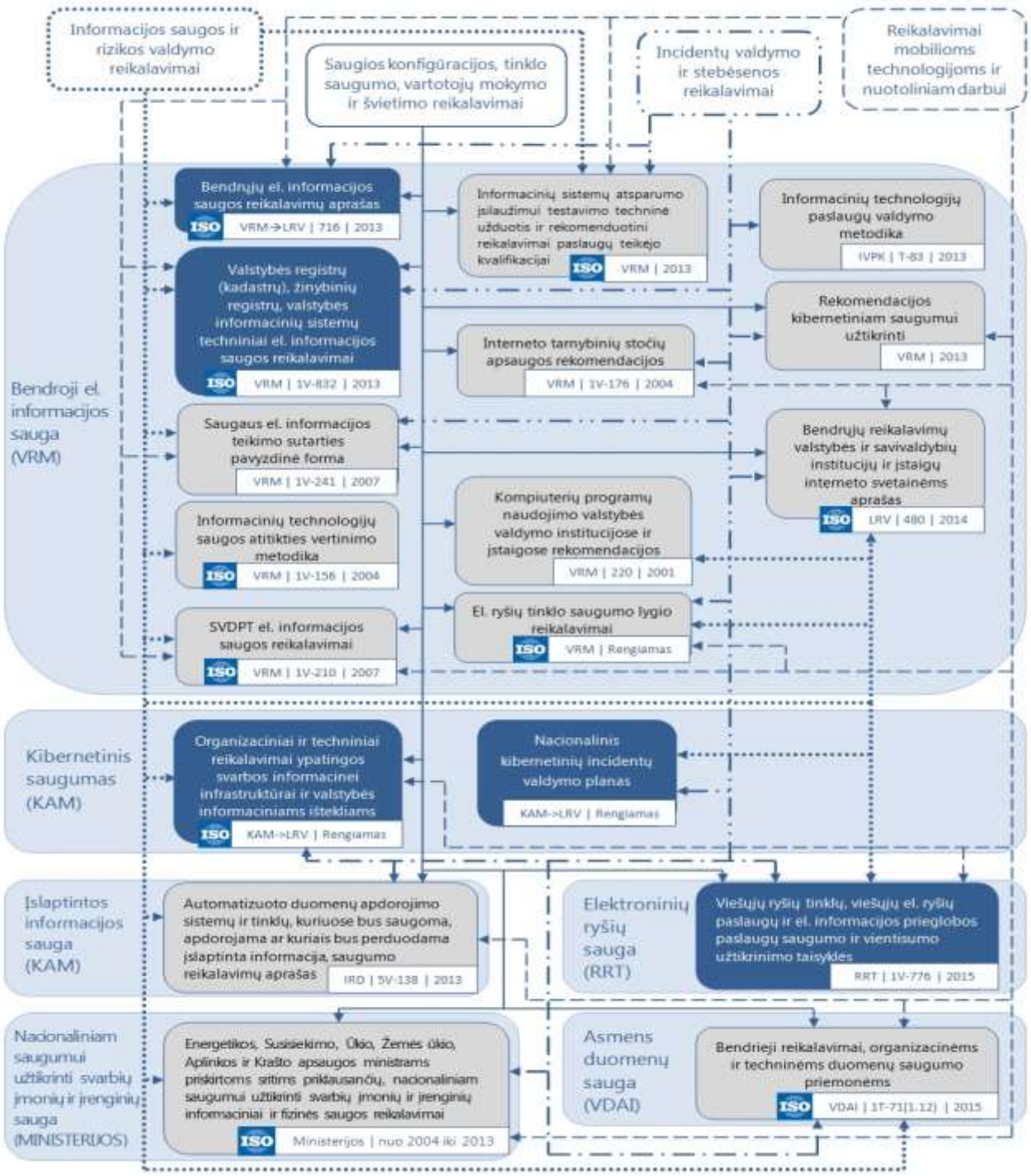
tikrintų įstaigų nurodyti kibernetinio saugumo ir el. informacijos saugos reglamentavimo trūkumai.

* KAM 2015-11-19 pateikė LRV nutarimo „Dėl Nacionalinio kibernetinių incidentų valdymo plano patvirtinimo“ projektą.

Šaltinis – Valstybės kontrolė.

Išanalizavę Kibernetinio saugumo įstatymui įgyvendinti reikalingų teisės aktų rengimo planą, nustatėme, kad nenumatyta peržiūrėti visų iki šiol galiojančių su el. informacijos sauga susijusių reikalavimų, nors yra tokių, kurie savo reikšme ar turiniu apima vienodas informacijos saugos valdymo ir kontrolės priemones, galioja ir nėra atnaujinti nuo 2001 m., taigi praranda aktualumą ir turėtų būti keistini (detaliau žr. 5 pav.).

5 pav. Kibernetinio saugumo ir el. informacijos saugos reikalavimų rengimo apimtys ir sąsajos.



ISO – teisės aktai rengti atsižvelgiant į ISO 27000 šeimos standartų rekomendacijas.

– įgyvendinant Kibernetinio saugumo įstatymą numatyti parengti, peržiūrėti teisės aktai.

– kiti teisės aktai, kurių nenumatyta peržiūrėti ar panaikinti įsigaliojus Kibernetinio saugumo įstatymui.

Šaltinis – Valstybės kontrolė.

Kol informacijos saugos reikalavimus įvairiais aspektais nustatančios įstaigos nesutars dėl kibernetinio saugumo, el. informacijos saugos ir kitų su informacijos sauga susijusių sričių reikalavimų suderinimo, naujų reikalavimų rengimas ir dalinis esamų reikalavimų tobulinimas negali užtikrinti, kad valstybėje bus panaikinti pertekliniai ir nustatyti tarpusavyje suderinti įvairių sričių el. informacijos saugos reikalavimai, sumažinta administracinė našta šiuos reikalavimus įgyvendinančioms ir jų įgyvendinimą stebinčioms įstaigoms. Tai, kad valstybėje neplanuojama nustatyti reikalavimų, kurie apimtų vieną tikslą, reikšmę ar turinį ir peržiūrėti visų iki šiol galiojančių

teisės aktų, reglamentuojančių informacinių išteklių, informacinių technologijų priemonių valdymą ir saugą, pastebėjome ir 2013 m. atlikę „Valstybės informacinių išteklių valdymo" auditą.

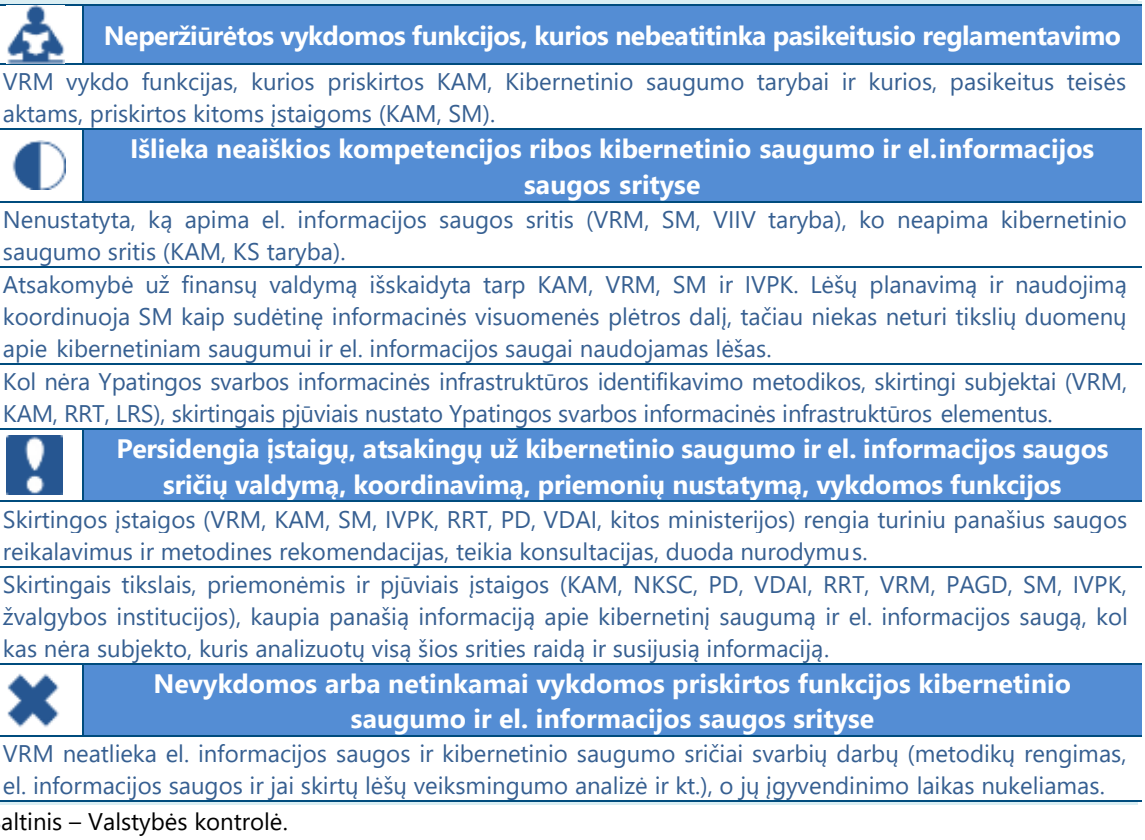
Siekiant sudaryti sąlygas nuosekliam kibernetinio saugumo ir kitų el. informacijos saugos sričių reglamentavimui, tikslinga skirti koordinatorių, kuris valstybės mastu koordinuotų šių sričių reikalavimų rengimą, jų suvienijimą. Taip pat papildyti įstatymų įgyvendinančių teisės aktų rengimo planus nuostatomis dėl šių sričių esamų teisės aktų peržiūros, jų suderinimo, trūkstamų nuostatų ir metodinių dokumentų patvirtinimo. Tai padėtų užtikrinti veiksmingą kibernetinio saugumo ir el. informacijos saugos reikalavimų rengimą, operatyviau reaguoti į probleminius klausimus, pokyčius ir naujus iššūkius, rengiant reikalavimus, metodinius dokumentus ir skelbiant įvairių sričių el. informacijos saugos valdymo praktiką.

1.3. Nebaigta formuoti kibernetinio saugumo ir el. informacijos saugos organizacinė struktūra ir valdymas

Išnagrinėję kibernetinio saugumo ir el. informacijos saugos politiką formuojančių ir įgyvendinančių įstaigų tarpusavio ryšius ir vykdomas funkcijas, nustatėme, kad 2015 m. pradėjo veikti kibernetinio saugumo valdymo sistema, tačiau ji nesudaro visų su el. informacijos sauga susijusių sričių darnaus valdymo sąlygų.

Kibernetinio saugumo įstatyme[35] apibrėžtos kibernetinio saugumo politiką formuojančios ir įgyvendinančios institucijos, jų įgaliojimai, tačiau iš tiesų kol kas neišvengiama dalinio įstaigų veiklos dubliavimo, trūksta kompetencijos atskyrimo formuojant ir įgyvendinant kibernetinio saugumo ir el. informacijos saugos politiką, neperžiūrėtos vykdomos funkcijos, kurios nebeatitinka pasikeitusio reglamentavimo (žr. 6 pav., detaliau 3 priede).

6 pav. Kibernetinio saugumo ir el. informacijos saugos politiką formuojančių ir įgyvendinančių institucijų tarpusavio ryšiai ir vykdomos funkcijos.



Šaltinis – Valstybės kontrolė.

[35] Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014-12-11 Nr. XII-1428, 2 skyrius.

Kuo daugiau įstaigų yra atsakingos už el. informacijos saugos sričių valdymą, koordinavimą ir priemonių nustatymą, tuo sudėtingiau šioje srityje formuoti nuoseklią valstybės valdymo politiką, suderinti skirtingų institucijų valdymo interesus, užtikrinti tinkamą lėšų panaudojimą.

Seimo Informacinės visuomenės plėtros komitetas 2012 m. pareiškė susirūpinimą Vidaus reikalų ministerijos netinkamu, nepakankamu ir neatsakingu funkcijų vykdymu formuojant valstybės politiką el. informacijos saugos (kibernetinio saugumo) srityje, organizuojant, koordinuojant ir kontroliuojant jos įgyvendinimą[36]. Pažymėtina, kad, iki šiol, ministerija bendrosios el. informacijos saugos, kuri yra kitų el. informacijos saugos sričių (taip pat ir kibernetinio saugumo) pagrindas, valdymui skiria nepakankamai dėmesio (peržiūrėti ne visi bendrieji ir techniniai el. informacijos saugos reikalavimai, neperžiūrėta valstybės el. informacijos saugos valdymo struktūra (komisijos, tarybos, valdymo grupės), neatliekami kiti suplanuoti šios srities reglamentavimo tobulinimo, skiriamų lėšų naudojimo, grėsmių ir pažeidžiamumų vertinimo darbai), todėl yra didelė rizika, kad viešajame sektoriuje nebus užtikrintas pakankamas el. informacijos saugos koordinavimas ir reikalavimų įgyvendinimas.

Siekiant suderinti kibernetinio saugumo ir el. informacijos saugos politikos formavimo ir įgyvendinimo kryptis, viešajame sektoriuje tikslinga optimizuoti šių sričių valdymą – parengti valstybės el. informacijos saugos valdymo konsolidavimo planą. Tokiu būdu viešasis sektorius artėtų prie centralizuoto šių sričių valdymo, reikalavimų rengimo, analizės, lėšų, skiriamų kibernetinio saugumo ir el. informacijos saugos priemonėms kurti ir palaikyti, kontrolės.

1.4. Kibernetinio saugumo ir el. informacijos saugos finansų valdymas nepakankamai veiksmingas

Kibernetiniam saugumui ir el. informacijos saugai užtikrinti skiriamos valstybės biudžeto asignavimų, ES ir kitos tarptautinės finansinės paramos lėšos. Susisiekimo ministerija koordinuoja informacinės visuomenės plėtros lėšų planavimą ir naudojimą, tačiau kibernetiniam saugumui ir el. informacijos saugai reikalingų lėšų skyrimo prioritetai ir kriterijai nenumatyti.

Informacinių technologijų saugai skirta 11,93 mln. EUR[37] 2007–2013 m. ES struktūrinės paramos lėšų. Audito metu nustatėme, kad įstaigos gerino saugos būklę panaudodamos ir kitas šio laikotarpio ES paramos lėšas[38] (žr. pavyzdį).

[36] Lietuvos Respublikos Seimo Informacinės visuomenės plėtros komiteto 2012-09-19 posėdžio Nr. 280-P-26 protokolas.

[37] Sudarytos septynios sutartys, lėšos skirtos Muitinės departamento, Registrų centro, Centrinės hipotekos įstaigos, Valstybinės mokesčių inspekcijos, Vidaus reikalų ministerijos, Gyventojų registro tarnybos, Valstybinio socialinio draudimo fondo valdybos ir Valstybės saugumo departamento saugai gerinti.

[38] ES struktūrinės paramos 2007–2013 m. Žmogiškųjų išteklių plėtros veiksmų programos „Administracinių gebėjimų stiprinimo ir viešojo administravimo efektyvumo didinimas“ prioriteto „VP1-4.3-VRM-01-V Viešųjų paslaugų kokybės iniciatyvos“ priemonės lėšomis Informacijos saugumo valdymo sistemų (ISVS) diegimas – viešajame sektoriuje – Aplinkos ministerijoje, Asmens dokumentų išrašymo centre, Gyventojų registro tarnyboje, Ginklų fonde; „VP1-4.2-VRM-01-V Veiklos valdymo tobulinimas“ priemonės lėšomis LINESIS diegimas – tobulinimas, „VP1-4.2-VRM-03-V Viešojo administravimo subjektų sistemos tobulinimas“ priemonės lėšomis (Krašto apsaugos ministerijos ryšių ir informacinių sistemų tobulinimas) ir kt.

Pavyzdys

Švietimo ir mokslo ministerija el. informacijos saugos ir kibernetinio saugumo klausimus sprendžia kuriant, aptarnaujant ir plėtojant valstybės registrus ir informacines sistemas. Nuo 2009 m. pagrindinis šių investicijų finansavimo šaltinis yra ES fondai, kurių priemones[39] administruoja pati ministerija. Įgyvendinant projektus už 282 tūkst. EUR įsigyta programinė įranga skirta spręsti el. informacijos saugos ir kibernetinio saugumo problemas. Švietimo ir mokslo ministerijos administruojamų priemonių projektų nevertino institucijos, atsakingos už informacinės visuomenės plėtrą (Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos), jų nereikia derinti su Krašto apsaugos ministerija (kibernetinio saugumo politikos formuotoja), Vidaus reikalų ministerija (formuojančia valstybės informacinių išteklių saugos politiką).

Dėl minėtų priežasčių nė viena institucija neturi tikslių duomenų, kiek skirta ir panaudota ES paramos lėšų valstybės institucijų kibernetiniam saugumui ir el. informacijos saugai gerinti, nėra galimybės pamatuoti ir įvertinti, kaip pasikeitė įstaigų kibernetinio saugumo ir el. informacijos saugos būklė, panaudojus šias lėšas.

Išanalizavę El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programos įgyvendinančių institucijų pateiktus duomenis nustatėme, kad kibernetiniam saugumui ir el. informacijos saugai planuojamos lėšos valstybės ir instituciniu mastu taip pat neskaičiuojamos, o valstybės institucijos kibernetinio saugumo ir el. informacijos saugos priemones planuoja kartu su informacinių technologijų plėtros ar kitomis veiklomis, todėl tikslių duomenų apie šiai sričiai naudojamas lėšas neturi.

Vidaus reikalų ministerija, renkanti ir analizuojanti informaciją apie institucijų valdomų valstybės informacinių išteklių saugą ir tam naudojamas lėšas[40], turėjo sukurti lėšų, skiriamų informacinių išteklių plėtrai, palaikymui ir saugai, kontrolės mechanizmą, teikti Vyriausybei ir institucijoms pasiūlymus dėl lėšų valstybės informacinių išteklių saugai efektyvesnio naudojimo, tačiau šių darbų neatliko.

Taigi nei Vidaus reikalų ministerija, nei Krašto apsaugos ministerija (nuo 2015 m. pradėjusi formuoti kibernetinio saugumo politiką) neturi tikslių duomenų apie vykdomus kibernetinio saugumo ir el. informacijos saugos projektus (jų turinį ir skaičių) ir informacijos, kiek valstybės mastu planuota, skirta ir panaudota lėšų šios srities būklei gerinti.

Krašto apsaugos ministerijos nuomonė[41]

Kibernetinio saugumo priemonių diegimas yra neatsiejamas nuo saugomų informacinių išteklių ir informacinės infrastruktūros plėtros, o dažnai yra ryšių ir informacinių sistemų (toliau – RIS) integrali dalis, tad manome, jog investicijų, skiriamų RIS plėtrai ir jų kibernetiniam saugumui dauguma atvejų neįmanoma išskirti. Kibernetiniam saugumui skirtos lėšos galėtų būti aiškiai atskiriamos tais atvejais, kai planuojama įsigyti specializuotas kibernetinio saugumo sistemas ar priemones, kurios nėra integralios informacinių išteklių ir informacinės infrastruktūros dalis. Atkreipiame dėmesį, jog KSĮ nustato, kad valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros valdytojai privalo savo lėšomis užtikrinti savo valdomų išteklių ir infrastruktūros atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams, tad manome, kad centralizuotas kibernetiniam saugumui reikalingų lėšų planavimas nėra tikslingas, o daugeliu atveju nėra įmanomas. Manome, kad tikslingiau yra kontroliuoti kibernetinio saugumo priemonių įgyvendinimą ir kibernetinio saugumo užtikrinimą, nei atskiras lėšas kibernetiniam saugumui užtikrinti.

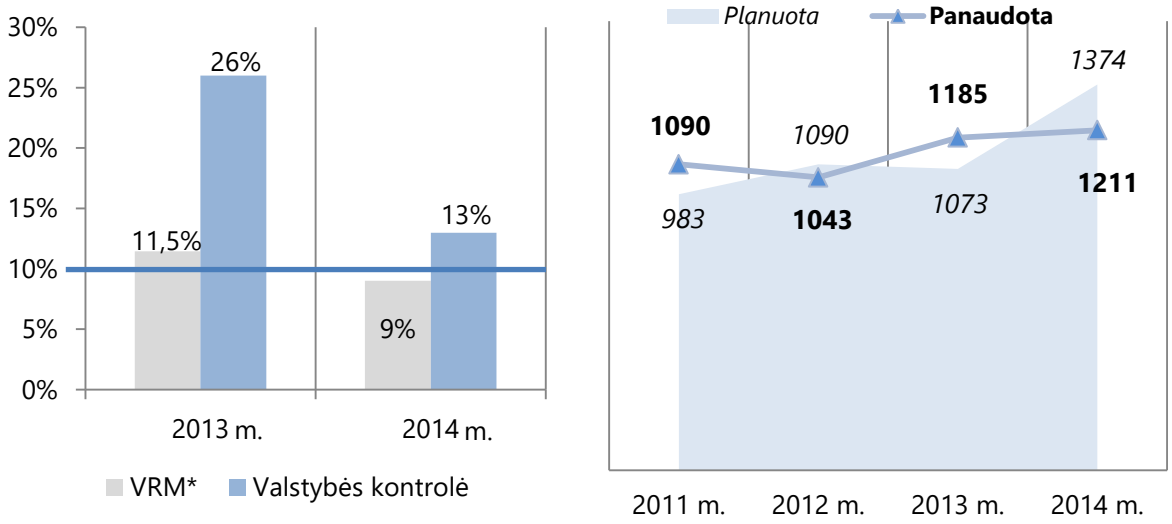
[39] ES struktūrinės paramos 2007–2013 m. 1.2 programos, 1.2 prioriteto „Mokymasis visą gyvenimą“ priemonės: VP1-2.1-ŠMM-03-V Švietimo personalo (administravimo personalo, švietimo vadybininkų) kvalifikacijos tobulinimo sistemų plėtra, VP1-2.1-ŠMM-02-V Lyderyste paremtas ir lyderiavimą skatinantis švietimo įstaigų valdymo tobulinimas, VP1-2.2-ŠMM-04-V Aukščiausios kokybės formaliojo ir neformaliojo mokymo paslaugų teikimas.

[40] Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807, 5 str. 4 d. 2 p.

[41] Lietuvos Respublikos krašto apsaugos ministerijos 2015-12-09 raštas Nr. 12-01-2369.

El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programoje 2015 m. siekta informacinių sistemų saugai skirti 10 proc. (2019 m. – 15 proc.)[42] visų lėšų, planuojamų skirti informacinių sistemų plėtrai ir palaikymui. Audito metu surinkti duomenys rodo, kad investicijos į saugos priemones jau keletą metų viršija šį rodiklį, o šiai sričiai skiriamos lėšos kasmet auga: vidutiniškai skiriama apie 1,13 mln. EUR (žr. 7 pav.).

7 pav. Išlaidų, skirtų kibernetiniam saugumui ir el. informacijos saugai užtikrinti, pokyčiai 2011–2014 m. (tūkst. EUR).



* VRM duomenimis 2014 m. valstybės įstaigos ir savivaldybės vidutiniškai skyrė 9 proc. viso informacinių technologijų plėtrai ir palaikymui skirto biudžeto (2013 m. – 11,46 proc.). Valstybės institucijų Valstybės kontrolei šio laikotarpio pateikti duomenys skiriasi nuo tų, kurie pateikti VRM: 2013 m. sudaro 26 proc., 2014 m. – 13 proc., kai kurių įstaigų atvejais 60–85 proc. viso informacinių technologijų biudžeto.

Šaltinis – Valstybės kontrolė pagal Vidaus reikalų ministerijos ir institucijų patikros duomenis.

Minėtą programą įgyvendinančių įstaigų pateiktais duomenimis, gerinant kibernetinio saugumo ir el. informacijos saugos būklę 2011–2014 m. panaudota 20,9 mln. EUR.

Susisiekimo ministerijos ir Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos duomenimis, 2015 m. valstybės kapitalo investicijos šiai sričiai sudarys 0,8 mln. EUR, o planuojant 2014–2020 m. ES fondų investicijų lėšas valstybės informacinės infrastruktūros ir išteklių saugai numatyta skirti dar 14,8 mln. EUR.

Iš viso susidaro 36,5 mln. EUR lėšų suma, kurią valstybė skiria kibernetinio saugumo ir el. informacijos saugos būklei gerinti (žr. 8 pav.).

8 pav. Kibernetinio saugumo ir el. informacijos saugos būklei gerinti skiriamos lėšos.

* VKI – Valstybės kapitalo investicijos.

Šaltinis – Valstybės kontrolė pagal Vidaus reikalų ministerijos, Susisiekimo ministerijos, Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos ir patikrų duomenis.

[42] Lietuvos Respublikos Vyriausybės 2011-06-29 nutarimu Nr. 796 patvirtintos Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos įgyvendinimo priedo 18 p.

Pažymėtina, kad faktinės viešojo sektoriaus įstaigų išlaidos, tenkančios kibernetinio saugumo ir el. informacijos saugos sričiai, yra didesnės nei nurodyta 8 pav., nes tik 21 proc. visų panaudotų lėšų audito metu tikrintos įstaigos galėjo detalizuoti išlaidas pagal veiklas ar metus. Be to, įstaigos, siekdamos užtikrinti savo valdomos infrastruktūros saugą, finansavimo projektams naudoja šaltinius, kurių lėšų ir veiklų pagrįstumo neįvertina kompetentingos institucijos. Kai kuriais atvejais tokios suplanuotos lėšos (vertė) siekia 43 proc. (6,37 mln. EUR) visų valstybės mastu planuojamų 2014–2020 m. ES fondų investicijų į valstybės informacinės infrastruktūros ir išteklių saugą (14,8 mln. EUR).

Pavyzdys

Vyriausybė 2015 m. rugsėjo 10 d. pritarė[43] Energetikos ministerijos siūlymui Lietuvos elektros perdavimo sistemos operatoriaus elektros perdavimo Sistemos valdymo ir Duomenų centro saugos projektą pripažinti valstybei svarbiu ekonominiu projektu. Konsultantų padedama įvertinusi šios infrastruktūros saugą, Energetikos ministerija ją įvardijo kaip ypatingos svarbos infrastruktūrą (nors tokios infrastruktūros identifikavimo metodiką ir jos valdytojų sąrašą rengia Vidaus reikalų ministerija, o tvirtina Vyriausybė) ir, siekdama gerinti esamą būklę ir įgyvendinti Kibernetinio saugumo įstatymą, prašė 6,37 mln. EUR. Šio nutarimo projekto medžiaga su Krašto apsaugos ministerija (kibernetinio saugumo politikos formuotoja) nederinta.

Tokiu būdu planuojamų lėšų nemato kibernetinio saugumo politikos formuotojas, šios srities finansus kontroliuojančios įstaigos ir niekas nekontroliuoja, ar įstaigų vykdomos veiklos atitinka nacionaliniu mastu formuojamas kibernetinio saugumo ir el. informacijos saugos užtikrinimo kryptis, koks šių lėšų panaudojimo efektyvumas visos valstybės mastu.

Nustačius kibernetinio saugumo ir el. informacijos saugos lėšų skyrimo ir panaudojimo prioritetus ir kriterijus, atsirastų galimybė įvertinti visų šiam tikslui skiriamų lėšų suderinamumą su vykdoma politika. Politikos formuotojas žinotų įstaigų kibernetinio saugumo ir el. informacijos saugos būklę, ar lėšos naudojamos pagal paskirtį; taip pat galėtų kaupti duomenis apie tai, kam konkrečiai naudojamos lėšos (pvz.: programinė, techninė įranga, mokymai ir kt.), įvertinti ir nustatyti trūkumus, kuriuos būtina šalinti.

[43] Lietuvos Respublikos Vyriausybės 2015-09-10 nutarimo Nr. 972 „Dėl LITGRID AB elektros perdavimo sistemos valdymo ir duomenų centro saugos projekto pripažinimo valstybei svarbiu ekonominiu projektu“ 1 p.

2. VALSTYBINĖSE ĮSTAIGOSE TAIKOMOS KIBERNETINIO SAUGUMO TECHNINĖS IR ORGANIZACINĖS PRIEMONĖS TURI TRŪKUMŲ ARBA NEĮGYVENDINAMOS

Audito metu nebuvo patvirtinti Kibernetinio saugumo įstatyme įvardyti organizaciniai ir techniniai reikalavimai, taikytini ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, todėl, siekdami nustatyti, kaip viešajame sektoriuje užtikrinamas kibernetinis saugumas, nagrinėjome tai, kiek valstybinėse įstaigose taikomos priemonės atitinka pripažintas šios srities gerosios valdymo praktikos rekomendacijas ir kaip įgyvendinami esami el. informacijos saugos reikalavimai (plačiau žr. 2 priedą).

Laikėmės nuomonės, kad kibernetinis saugumas valstybinėse įstaigose užtikrinamas, kai:

- nustatoma kibernetinio saugumo politika ir valdymo procedūros;
- įgyvendinamos kibernetinio saugumo techninės priemonės atitinka pripažintas šios srities gerosios valdymo praktikos rekomendacijas.

Audito metu tikrinome ministerijas ir tas įstaigas, kurios dalyvavo įgyvendinant El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programą[44]. Patikrų metu surinkome informaciją, kuri gali tiesiogiai ar netiesiogiai paveikti tikrintų įstaigų kibernetinio saugumo, el. informacijos saugos organizacinių ir techninių priemonių valdymo būklę, todėl ataskaitoje pateikiame apibendrintus gautų rezultatų vidurkius.

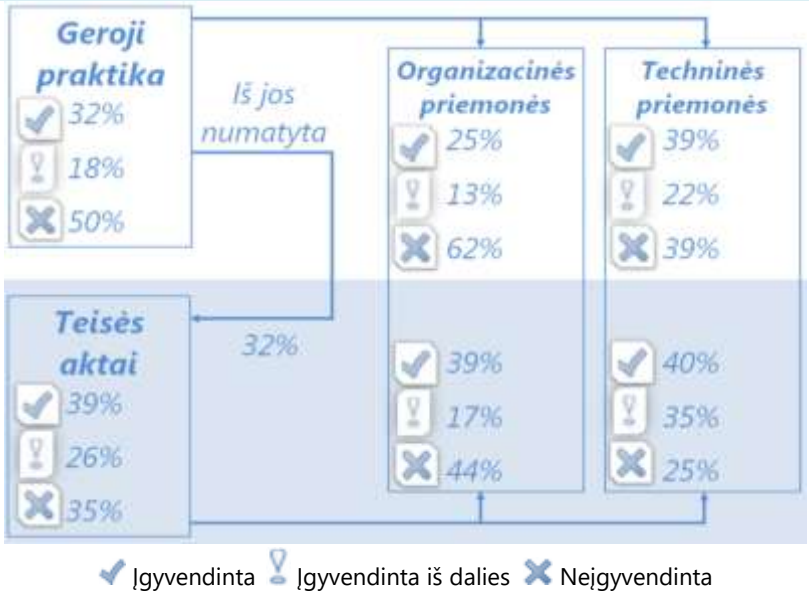
Išanalizavę 18-kos įstaigų patikrų vietoje rezultatus nustatėme, kad kibernetinio saugumo organizacinių ir techninių priemonių įgyvendinimas viešajame sektoriuje yra nepakankamas, nes šiose įstaigose vidutiniškai taikoma 25 proc. kibernetinei saugai užtikrinti rekomenduojamų organizacinių priemonių (13 proc. jų taikoma iš dalies) ir tinkamai įgyvendinama tik 39 proc. kibernetiniai saugai užtikrinti rekomenduojamų techninių priemonių (22 proc. jų įgyvendinama iš dalies) (žr. 9 pav.).

Pažymėtina, kad 32 proc. gerojoje praktikoje rekomenduojamų kibernetinio saugumo organizacinių ir techninių priemonių jau numatytos teisės aktuose, nustatančiuose el. informacijos saugos reikalavimus, tačiau tikrintos įstaigos tik 39 proc. esamų organizacinių saugos reikalavimų įgyvendina tinkamai (17 proc. įgyvendina iš dalies) ir tinkamai įgyvendina tik 40 proc. esamų techninių saugos reikalavimų (35 proc. įgyvendina iš dalies).

Dėl išvardytų priežasčių tikrintos valstybinės įstaigos nepakankamai pasiruošusios tinkamai reaguoti į kibernetinėje erdvėje kylančias grėsmes ir neužtikrina tokio el. informacijos saugumo lygio, kuris jau nustatytas teisės aktuose.

[44] Lietuvos Respublikos Vyriausybės 2011-06-29 nutarimu Nr. 796 patvirtintos Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos priede išvadintos institucijos, išskyrus Krašto apsaugos ministeriją, Lietuvos mokslo ir studijų institucijų kompiuterinio tinklo (LITNET) tarybą ir viešojo administravimo institucijas, teikiančias paslaugas kibernetinėje erdvėje.

9 pav. Patikrų vietoje rezultatų suvestinė.



Šaltinis – Valstybės kontrolė pagal patikrų vietoje duomenis.

Per patikras išryškėję pagrindiniai viešojo sektoriaus kibernetinio saugumo organizacinių ir techninių priemonių valdymo trūkumai pateikti 2 lentelėje. Nustatytų trūkumų skaičius yra didelis, todėl tik laiko klausimas, kada gerojoje praktikoje įvardytos tikėtinos pasekmės taps realybe ir sukels valstybei neigiamų padarinių.

2 lentelė. Viešojo sektoriaus kibernetinio saugumo organizacinių ir techninių priemonių valdymo trūkumai.

1 Saugumo valdymo sistema kuriama su trūkumais, dokumentacija rengiama, tačiau formaliai. *Tikėtinos pasekmės:* ** neefektyvus politikos įgyvendinimas;* ** minimali nauda iš investicijų į saugą;* ** nustatytose tolerancijos ribose nevaldoma rizika.*	0%	nustato biudžetą informacijos saugai;
		peržiūri / atnaujina saugos politiką įvykus saugumo incidentams;
	6%	nustato procedūras ir laiką pažeidžiamumui ištaisyti;
	22%	rengia saugumo tobulinimo planus;
		sudaro rizikos valdymo registrą ir jį nuolat atnaujina;
	33%	saugumo politikos nuostatas įtraukia į sutartis su trečiosiomis šalimis;
	39%	tikrina saugos procedūras, siekiant įsitikinti ar jų laikomasi;
	44%	suteikia įgaliojimus atsakingiems asmenims veikti visoje organizacijoje;
	56%	reguliariai (kas 12 mėn.) atlieka rizikos vertinimą;
2 Mobilių ir kitų technologijų ir prietaisų saugai užtikrinti skiriamas nepakankamas dėmesys. *Tikėtinos pasekmės:* ** informacijos nutekėjimas, praradimas;* ** įsilaužimai, saugios konfigūracijos sukompromitavimas.*	0%	jei leidžiama, naudoja priemones nešiojamoms laikmenoms valdyti;
	6%	turi asmeninių daiktų (*Bring your own device*) naudojimo tvarkas;
	22%	diegiant naujas technologijas atlieka rizikos vertinimą dėl jų naudojimo;
	50%	mobilius prietaisus, kurie naudojami darbui, apsaugo nuo neautorizuotos prieigos;
	60%	turi įdiegę antikenkėjišką programinę įrangą mobiliuose prietaisuose;
3 Trūksta atsakingo požiūrio į saugos incidentų valdymą ir veiklos tęstinumo užtikrinimą. *Tikėtinos pasekmės:* ** nesugebėjimas aptikti, reaguoti į atakas ir jas užkardyti;* ** pasikartojantys veiklos, operacijų sutrikimai;* ** finansinė žala, žala reputacijai.*	0%	saugos stebėsena susieta su incidentų valdymo procedūromis;
	6%	turi incidentui ištirti reikiamų įrodymų surinkimo procedūras;
	17%	incidentus klasifikuoja ir pagal tai numato jų valdymo procedūras;
		rengia veiklos tęstinumo ataskaitas, kuriose matosi planų efektyvumas;
	22%	reguliariai testuoja incidentų valdymo tvarkas ir veiklos tęstinumo valdymo planus;
	39%	analizuoja incidentus siekiant, kad jie nepasikartotų;
	44%	atnaujina veiklos tęstinumo valdymo planus;
	67%	reguliariai testuoja atsarginių kopijų būklę ir galimybes atstatyti iš atsarginių kopijų;

4 Silpnas vidinis personalo kompetencijos formavimas ir išorinis bendradarbiavimas. *Tikėtinos pasekmės:* ** saugumo incidentų skaičiaus didėjimas, jų tolerancija, vidinės grėsmės;* ** silpnos saugumą užtikrinančios procedūros, nepakankamas kontrolės priemonių užtikrinimas;* ** atsakomybės už neteisėtą veiklą išvengimas.*	0%	tikrina saugos komandos žinių lygį;
	11%	adaptuoja saugumo mokymus atsižvelgiant į darbinę aplinką;
	22%	teikia informaciją apie incidentus nacionaliniam CERT;
	28%	vertina darbuotojų keliamas grėsmes informacijos ir ryšių technologijoms;
	29%	reguliariai moko saugos komandą;
	50%	įstaigų perduoda neteisėtos ar kenkėjiškos veiklos įrodymus teisėsaugos institucijoms;
	56%	žino kam, kaip ir ką pranešti įvykus saugumo incidentui;
		reguliariai moko naudotojus informacijos saugos temomis;
5 Saugi konfigūracija ir tinklo saugumas nėra prioritetai užtikrinant el. informacijos saugą. *Tikėtinos pasekmės:* ** el. paslaugų sutrikdymas;* ** neautorizuoti pokyčiai sistemose;* ** jautrios informacijos nutekinimas, duomenų iškraipymas, įrangos sugadinimas;* ** piktnaudžiavimas privilegijomis;* ** įdiegtų saugumo kontrolės priemonių panaikinimas;* ** nesaugios sistemų konfigūracijos, neatnaujintų ar pažeidžiamų sistemų išnaudojimas;* ** kenksmingo programinio kodo patekimas ir plitimas.*	0%	analizuoja jei vartotojas dirba ne iš savo darbo vietos darbe;
	6%	draudžia sistemos darbui nereikalingas funkcijas ir prietaisus;
		analizuoja audito įrašus dėl administratorių netipinės veiklos;
		nustato ir dokumentuoja visos naudojamos techninės ir programinės įrangos minimalų saugumo reikalavimų rinkinį (*base line*).
	11%	atnaujinimus įdiegia daugiau nei per 30 d. nuo jų pasirodymo;
	17%	turi tvarkas, kuriomis suteikiamos administratoriaus paskyros;
		kritinius atnaujinimus įdiegia per 2 d. nuo jų pasirodymo;
		atsargines kopijas šifruoja kai jos yra tinkle arba perkeliamos į debesį;
	22%	diegiant programinę įrangą įsitikina, kad ji saugi ir tinkama naudoti;
		blokuoja administratoriaus paskyras lokaliuose kompiuteriuose;
		nustato, kokios paslaugos (*network ports/protocols*) leidžiamos / draudžiamos naudoti;
	24%	tinkamai saugo sistemų audito įrašus;
	28%	stebi visų kritinių bylų vientisumą;
		kritinių įrenginių administravimui naudoja papildomą autentifikavimą;
	33%	turi konfigūracijos valdymo / pokyčių valdymo procedūras;
	38%	išorinio perimetro ugniasienės slaptažodžius keičia ne rečiau kaip per 60d.;
	39%	analizuoja audito įrašus dėl naudotojų netipinės veiklos;
		tikrinimo metu neturėjo tinklo paslaugų (*network ports/protocols*), kurioms nereikalinga prieiga prie interneto;
	44%	turi nustatę leistinos naudoti programinės įrangos sąrašą;
		tikrinimo metu neturėjo neatpažintų įrenginių tinkle;
		programinės įrangos atnaujinimus išbando testinėje aplinkoje;
	47%	naudoja tinklo protokolus (pvz.: Telnet, RDP ir kt.) be papildomos apsaugos (*SSL, IPSEC*);
	50%	tikrina faktinę naudojamų tinklo paslaugų būklę;
		tikrinimo metu turėjo aktyvių nenaudojamų paskyrų;

Šaltinis – Valstybės kontrolė pagal patikrų vietoje duomenis.

Rengdamos kibernetinio saugumo ir el. informacijos saugos reikalavimus bei šios srities metodinius dokumentus, Krašto apsaugos ministerija ir Vidaus reikalų ministerija turėtų atkreipti dėmesį į praktinius viešojo sektoriaus organizacinių ir techninių priemonių valdymo trūkumus ir, juos išanalizavusios, įtraukti ir (arba) papildyti šios srities nuostatas dėl saugumo valdymo sistemos kūrimo, mobilių ir kitų technologijų naudojimo, incidentų valdymo, personalo kompetencijos tobulinimo, išorinio bendradarbiavimo, veiklos tęstinumo, saugios konfigūracijos ir tinklo saugumo užtikrinimo.

Be to, būtų tikslinga daugiau dėmesio skirti aktyviai konsultacinei veiklai: padėti kibernetinį saugumą ir el. informacijos saugą užtikrinantiems dalyviams tinkamai įgyvendinti šiai sričiai keliamus reikalavimus ir rekomendacijas.

Informacinių sistemų ir infrastruktūros audito departamento
direktorius Dainius Jakimavičius

Informacinių sistemų ir infrastruktūros audito departamento
Informacinių sistemų audito skyriaus
vyriausiasis valstybinis auditorius Rimgaudas Gamulis

Valstybinio audito ataskaitos kopijos pateiktos:

Lietuvos Respublikos Prezidento kanceliarijai, 1 egz.

Lietuvos Respublikos Seimo Audito komitetui, 1 egz.

Lietuvos Respublikos Seimo Informacinės visuomenės plėtros komitetui, 1 egz.

Lietuvos Respublikos Seimo Nacionalinio saugumo ir gynybos komitetui, 1 egz.

Lietuvos Respublikos Vyriausybės kanceliarijai, 1 egz.

Lietuvos Respublikos vidaus reikalų ministerijai, 1 egz.

Lietuvos Respublikos krašto apsaugos ministerijai, 1 egz.

Auditas atliktas, vykdant 2014-12-09 pavedimą Nr. P-90-4 ir 2015-04-08 pavedimą Nr. P-90-4-3

Auditą atliko valstybinių auditorių grupė:

Rimgaudas Gamulis (grupės vadovas)

Kęstutis Kumetaitis

Donatas Vitkus (iki 2015-06-09)

PRIEDAI

Valstybinio audito ataskaitos
„Kibernetinis saugumas Lietuvoje“
1 priedas

Rekomendacijų įgyvendinimo planas

Nr.	Rekomendacija	Subjektas, kuriam pateikta rekomendacija	Priemonės*	Rekomendacijos įgyvendinimo terminas (data)*
1.	Siekiant užtikrinti kibernetinį saugumą ir jo atsparumo didinimą, tobulinti esamą planavimą, teisinį reguliavimą ir finansų valdymą:			
1.1.	nustatyti bendras kibernetinio saugumo, el. informacijos saugos strategines kryptis ir joms pasiekti būtinas priemones;	Vyriausybė Krašto apsaugos ministerijos ir Vidaus reikalų ministerijos teikimu	1.1.1. Peržiūrėti El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programą ir patvirtinti naują strateginį dokumentą nustatantį bendras kibernetinio saugumo, el. informacijos saugos strategines kryptis.	2016 m. IV ketv.
			1.1.2. Patvirtinus 1.1.1. p. numatytą dokumentą, patikslinti kitus susijusius planavimo dokumentus (nurodytus ataskaitos 3 pav.).	2017 m. II ketv.
1.2.	skirti įstaigą, kuri valstybės mastu koordinuotų kibernetinio saugumo, el. informacijos saugos reikalavimų rengimą, jų suvienijimą;	Vyriausybė Krašto apsaugos ministerijos ir Vidaus reikalų ministerijos teikimu	1.2.1. Peržiūrėti ir patikslinti nutarimo dėl ministrams pavedamų valdymo sričių nuostatas, susijusias su kibernetiniu saugumu ir el. informacijos sauga, KAM ir VRM nuostatus.	2016 m. II ketv.
			1.2.2. Pavesti paskirtai įstaigai ir reikalavimus nustatančiom įstaigoms atlikti kibernetinio saugumo, el. informacijos saugos reikalavimų suvienijimą.	2017 m. IV ketv.
1.3.	konsoliduoti el. informacijos saugos valdymą;	Vyriausybė Krašto apsaugos ministerijos ir Vidaus reikalų ministerijos teikimu	1.3.1. Patvirtinti kibernetinio saugumo ir el. informacijos saugos valdymo susiejimo planą.	2017 m. III ketv.
			1.3.2. Priimti sprendimus dėl kibernetinio saugumo ir el. informacijos saugos valdymo konsolidavimo išnaudojant esamą situaciją ir turimus rezervus.	2017 m. III ketv.
			1.3.3 Sukurti kibernetinio saugumo dalyvių konsultavimo mechanizmą.	2016 m. III -IV ketv.
			1.3.4. Sukūrus mechanizmą (1.3.3.) įpareigoti įstaigas kaupti ir nuolat atnaujinti kibernetinio saugumo ir el. informacijos saugos žinių bazę.	2016 m. IV ketv.
1.4.	valstybės mastu nustatyti kibernetiniam saugumui, el. informacijos saugai reikalingų lėšų skyrimo ir panaudojimo prioritetus, kriterijus, stebėsenos ir kontrolės mechanizmą.	Vyriausybė Krašto apsaugos ministerijos ir Vidaus reikalų ministerijos teikimu	1.4.1. Priimti sprendimus dėl kibernetiniam saugumui ir el. informacijos saugai reikalingų lėšų naudojimo prioritetų, rekomenduojant juos įtraukti į reikalavimus dėl skiriamų lėšų naudojimo.	2016 m. I ketv.
			1.4.2 Nuostatas dėl kibernetinio saugumo ir el. informacijos saugos reikalingų lėšų skyrimo ir panaudojimo prioritetinių krypčių, kriterijų ir kontrolės mechanizmo įtraukti į 1.1.1. p. numatytą naują strateginį dokumentą.	2016 m. IV ketv.
			1.4.3. Vadovaujantis strateginiame dokumente nustatytomis prioritetinėmis kryptimis konkrečius kibernetinio saugumo ir el. informacijos saugos prioritetus, taip pat informaciją apie šios srities finansavimo planavimą ir panaudojimą periodiškai pateikti apsvarstyti Vyriausybei.	2017 m. II ketv.

Nr.	Rekomendacija	Subjektas, kuriam pateikta rekomendacija	Priemonės*	Rekomendacijos įgyvendinimo terminas (data)*
2.	Siekiant gerinti kibernetinio saugumo reglamentavimo kokybę ir efektyvumą, mažinti administracinę naštą šiuos reikalavimus įgyvendinančioms ir jų įgyvendinimą stebinčioms įstaigoms:			
2.1.	peržiūrėti esamus kibernetinio saugumo, el. informacijos saugos reikalavimus, juos suderinti ir (arba) patvirtinti trūkstamas nuostatas ir metodinius dokumentus;	Krašto apsaugos ministerija ir Vidaus reikalų ministerija	2.1.1. Atsižvelgiant į patikslintą kompetenciją kibernetinio saugumo ir el. informacijos saugos srityje atitinkamos ministerijos turi peržiūrėti esamus kibernetinio saugumo, el. informacijos saugos reikalavimus, juos suderinti ir patvirtinti trūkstamas nuostatas ir metodinius dokumentus.	2016 m. IV ketv.
2.2.	užtikrinti įstaigų konsultavimą ir informavimą kibernetinio saugumo ir el. informacijos saugos (valdymo sistemos kūrimas, incidentų valdymas, veiklos tęstinumo užtikrinimas, personalo kompetencijos tobulinimas, išorinis bendradarbiavimas, saugios konfigūracijos nustatymas, tinklo saugumas, mobilių ir kitų technologijų valdymas) klausimais.	Krašto apsaugos ministerija	2.2.1. Ne rečiau kaip kartą per metus apklausti kibernetinio saugumo dalyvius apie faktinę kibernetinio saugumo ir el. informacijos saugos konsultavimo būklę, gautos informacijos pagrindu aktualizuoti sukauptus žinių bazės duomenis.	Informacija už praėjusius metus vasario mėn. Vyriausybės kanceliarijai

* – priemones ir terminus rekomendacijoms įgyvendinti pateikė Lietuvos Respublikos Vyriausybės kanceliarija, Lietuvos Respublikos krašto apsaugos ministerija ir Lietuvos Respublikos vidaus reikalų ministerija.

Atstovai ryšiams, atsakingi už Valstybės kontrolės informavimą apie rekomendacijų įgyvendinimą plane nustatytais terminais:

Lietuvos Respublikos Vyriausybės kanceliarijos	
Nacionalinio saugumo ir krizių valdymo skyriaus vedėjas	Dalius Labanauskas
Viešojo valdymo ir socialinės apsaugos departamento Informacinės visuomenės skyriaus patarėjas	Edmundas Kazakevičius
Lietuvos Respublikos krašto apsaugos ministerijos	
Kibernetinio saugumo ir informacinių technologijų departamento	
Kibernetinio saugumo ir elektroninės informacijos saugos skyriaus patarėjas	Tomas Stamulis
Lietuvos Respublikos vidaus reikalų ministerijos	
Viešojo valdymo politikos departamento Viešojo administravimo politikos skyriaus vedėjas	Virginijus Vaškelis

Valstybinio audito ataskaitos
„Kibernetinis saugumas Lietuvoje“
2 priedas

Audito procedūros ir metodai

Nr.	Metodas	Tikslai
1.	Dokumentų peržiūra – nagrinėjome Vidaus reikalų ministerijos, Krašto apsaugos ministerijos, šių ministerijų valdymo srities įstaigų, kitų ministerijų, Vyriausybės kanceliarijos, Ryšių reguliavimo tarnybos, Valstybinės duomenų apsaugos inspekcijos, Valstybės saugumo departamento, Lietuvos mokslo ir studijų institucijų kompiuterinio tinklo (LITNET) tarybos ir Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos pateiktus dokumentus.	Išsiaiškinti ir nustatyti teisinio reglamentavimo, planavimo, funkcijų pasiskirstymo, finansų valdymo, ypatingos svarbos informacinės infrastruktūros identifikavimo trūkumus ir problemas el. informacijos saugos ir kibernetinio saugumo srityje.
2.	Pokalbiai su Vidaus reikalų ministerijos, Krašto apsaugos ministerijos, šių ministerijų valdymo srities įstaigų, kitų ministerijų, Vyriausybės kanceliarijos, Ryšių reguliavimo tarnybos, Valstybinės duomenų apsaugos inspekcijos, Valstybės saugumo departamento, Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos, asociacijos „INFOBALT“ atstovais.	
3.	Duomenų analizė ir skaičiavimas: ▪ El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programos įgyvendinimo būklės analizė; ▪ Kibernetinio saugumo įstatymui įgyvendinti reikalingų teisės aktų analizė; ▪ El. informacijos saugai ir kibernetiniam saugumui užtikrinti skiriamų valstybės biudžeto asignavimų, ES ir kitos tarptautinės finansinės paramos lėšų analizė; ▪ tikrintų įstaigų pateiktų duomenų analizė.	Nustatyti el. informacijos saugos ir kibernetinio saugumo teisės aktų rengimo trūkumus, El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programos, šios srities finansavimo pokyčius audituojamu laikotarpiu, pateikti konkrečius pavyzdžius audito ataskaitoje.
4.	Tikrinome ministerijas ir tas įstaigas, kurios dalyvavo įgyvendinant El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programą (pagal profesinį sprendimą atliktas aštuoniolikos valstybės įstaigų taikomų el. informacijos saugos ir kibernetinio saugumo organizacinių ir techninių priemonių vertinimas (analizuoti gauti dokumentai, įrodymai, atsakymai ir patikslinimai iš atsakingų valstybės įstaigos darbuotojų).	Nustatyti: – kaip įstaigų vadovybė valdo el. informacijos saugai ir kibernetiniam saugumui būdingą riziką, nustato politikos kryptis ir veiksmus; – kokios įgyvendinamos el. informacijos saugos ir kibernetinio saugumo organizacinės ir techninės priemonės; – kokie el. informacijos saugos ir kibernetinio saugumo klausimai aktualūs praktikoje; – sritis, kur el. informacijos saugos ir kibernetinio saugumo reglamentavimas turėtų būti tobulinamas. Pateikti gerąją praktiką ir konkrečius pavyzdžius audito ataskaitoje.
	Analizavome tikrintų įstaigų el. informacijos saugos ir kibernetinio saugumo priemonių atitiktį teisės aktų reikalavimams ir rekomendacijoms: Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas 2011-12-15 XI-1807; □ Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtinti Bendrųjų el. informacijos saugos reikalavimų aprašas, saugos dokumentų turinio gairių aprašas ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir el. informacijos svarbos nustatymo gairių aprašas; □ Vidaus reikalų ministro 2013-10-04 įsakymu Nr. 1V-832 patvirtinti Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų el. informacijos saugos reikalavimai; □ Vidaus reikalų ministro 2007-06-29 įsakymu Nr. 1V-241 patvirtinta Saugaus el. informacijos teikimo sutarties pavyzdinė forma; □ Vidaus reikalų ministro 2007-06-05 įsakymu Nr. 1V-210 patvirtinti Saugaus valstybinio duomenų perdavimo tinklo el. informacijos saugos reikalavimai; □ Vidaus reikalų ministro 2004-05-06 įsakymu Nr. 1V-156 patvirtinta Informacinių technologijų saugos atitikties vertinimo metodika; □ Vidaus reikalų ministro 2004-05-21 įsakymu Nr. 1V-176 patvirtintos Interneto tarnybinių stočių apsaugos rekomendacijos;	

Nr.	Metodas	Tikslai
5.	▫ Vidaus reikalų ministro 2001-05-09 įsakymu Nr. 220 patvirtintų Kompiuterių programų naudojimo valstybės valdymo institucijose ir įstaigose rekomendacijos; ▫ Vidaus reikalų ministerijos 2013 m. parengtos rekomendacijos kibernetiniam saugumui užtikrinti; ▫ Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2013-06-19 įsakymu Nr. T-83 patvirtinta Informacinių technologijų paslaugų valdymo metodika; Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas 1999-11-25 Nr. VIII-1443; ▫ Vyriausybės 2010-07-07 Nr. 1014 nutarimu patvirtintas Įslaptintai informacijai įrašyti skirtų laikmenų administravimo tvarkos aprašas; ▫ Informatikos ir ryšių departamento direktoriaus prie Vidaus reikalų ministerijos 2010-11-29 įsakymu Nr. 5V-138 patvirtinti Automatizuoto duomenų apdorojimo sistemų ir tinklų, kuriuose bus saugoma, apdorojama ar kuriais bus perduodama įslaptinta informacija, saugumo reikalavimų aprašas; Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, 1996-06-11 Nr. I-1374; ▫ Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008-11-12 įsakymu Nr. 1T-71 (1.12) patvirtinti Bendrieji reikalavimai organizacinėmis ir techninėms duomenų saugos priemonėms; Lietuvos Respublikos elektroninių ryšių įstatymas, 2004-04-15 Nr. IX-2135; ▫ Ryšių reguliavimo tarnybos direktoriaus 2011-10-21 Nr. 1V-1013 įsakymu patvirtintos Viešųjų ryšių tinklų, viešųjų el. ryšių paslaugų ir el. informacijos prieglobos paslaugų saugumo ir vientisumo užtikrinimo taisyklės. Užsienio praktikos apžvalga – nagrinėjome medžiagą susijusią su el. informacijos sauga ir kibernetiniu saugumu: ▫ Jungtinės Amerikos Valstijos (National Institute of Standards and Technology (NIST); Framework for Improving Critical Infrastructure Cybersecurity); ▫ Australija (Australian Government Information Security Manuals; Strategies to Mitigate Targeted Cyber Intrusions); ▫ Didžioji Britanija (Cyber Essentials Scheme: Requirements for basic technical protection from cyber attacks); ▫ Didžioji Britanija (10 Steps To Cyber Security; Information Assurance for Small and Medium Enterprises Consortium (IASME) Standards); ▫ Belgijos Karalystė (Belgian cyber security guide); ▫ Tarptautinė standartizacijos organizacija (ISO) (ISO 27000 series of standards); ▫ Tarptautinis informacijos saugumo forumas (ISF) (Standard of Good Practice for Information Security); ▫ SANS institutas (The Critical Security Controls for Effective Cyber Defense); ▫ Tarptautinė asociacija (ISACA) (European Cybersecurity Audit Assurance Programe; Transforming Cybersecurity).	

Valstybinio audito ataskaitos
„Kibernetinis saugumas Lietuvoje“
3 priedas

Kibernetinio saugumo ir el. informacijos saugos valdymo trūkumai

	Neperžiūrėtos vykdomos funkcijos, kurios nebeatitinka pasikeitusio reglamentavimo	
VRM	Nuostatai (LRV 2001-03-14 Nr. 291): • Formuoja valstybės politiką el. saugos, kibernetinio saugumo srityje, organizuoja, koordinuoja ir kontroliuoja jos įgyvendinimą (8.6 p.). • Koordinuoja valstybės institucijų ir įstaigų veiksmus įgyvendinant el. informacijos saugos (kibernetinio saugumo) valstybės institucijose ir įstaigose politiką (14.6 p.). • Atlieka saugos reikalavimų laikymosi priežiūrą (14.6 p.). • Konsultuoja [...] el. informacijos saugos (kibernetinio saugumo) klausimais (14.11 p.). • Rengia el. informacijos saugos (kibernetinio saugumo) reikalavimus, saugos dokumentų turinio gaires (14.10 p.).	Kiti teisės aktai: • El. informacijos saugos (kibernetinio saugumo) koordinavimo komisijos funkcijos (LRV 2006-12-13 Nr. 1266). • El. informacijos saugos (kibernetinio saugumo) konsultacinės tarybos funkcijos (VRM 2013-07-03 Nr. 1V-582). • Galimų kibernetinio saugumo incidentų pasekmių valdymo grupės veiklos funkcijos (VRM 2014-03-21 Nr. 1V-213). • Vykdo Saugumo priežiūros tarnybos funkcijas (VRM 2011-04-26 Nr. 1V-313 (8.4, 12.1-12.4 p.)). • Valdo Saugų valstybinį duomenų perdavimo tinklą ir skiria jo tvarkytoją (LRS 2011-12-15 Nr. XI-1807 (5 str. 4 d. 9 p.)).
	Išlieka neaiškios kompetencijos ribos kibernetinio saugumo ir el. informacijos saugos srityse	
Tarpinstitucinis koordinavimas	KAM	KSĮ (LRS 2014-12-11 Nr. XII-1428): • Formuoja kibernetinio saugumo valstybės politiką, organizuoja, koordinuoja ir kontroliuoja jos įgyvendinimą (6 str. 1 p.).
	KS Taryba	• Teikia pasiūlymus [...] dėl kibernetinio saugumo prioritetų, plėtros krypčių, siektinų rezultatų, jų įgyvendinimo būdų; dėl [...] bendradarbiavimo galimybių kibernetinio saugumo užtikrinimo srityje (9 str. 4 d. 1 ir 2 p.).
	VRM	Kiti teisės aktai: • Formuoja politiką valstybės informacinių išteklių saugos srityje tiek, kiek tai neapima kibernetinio saugumo (LRS 2011-12-15 Nr. XI-1807 (5 str. 4 d.)). • Koordinuoja El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programos įgyvendinimą (LRV 2001-03-14 Nr. 291 (14.7 p.)). • Kontroliuoja, kaip įgyvendinama el. informacijos saugos, kibernetinio saugumo srities valstybės politika ministerijai pavaldžiose įstaigose (LRV 2001-03-14 Nr. 291 (14.2 p.)). • Rengia valstybės politikos [...] saugos srityje įgyvendinimo strategiją, koordinuoja ir kontroliuoja jos įgyvendinimą (VRM 2015-06-30 Nr. 1V-534 (4.2.1. p.)).
	VIIV taryba	• Rengia pasiūlymus ir rekomendacijas Vyriausybei dėl [...] rekomenduojamų taikyti techninių reikalavimų (standartų) [...] saugos reikalavimų, saugos dokumentų turinio gairių, informacijos svarbos įvertinimo, [...] klasifikavimo pagal [...] informacijos svarbą kriterijus. (LRS 2011-12-15 Nr. XI-1807 (7 str. 2 d. 1 p.)) (LRV 2013-04-10 Nr. 307 (4. p.)).
	SM	• Rengia ir teikia pasiūlymus Vyriausybei dėl [...] informacijos ir ryšių technologijų tobulinimo ir plėtros krypčių, rekomenduojamų taikyti techninių reikalavimų (standartų) (LRS 2011-12-15 Nr. XI-1807 (5 str. 2 d. 1 p.)) (LRV 2010-10-13 Nr. 1480 (8.6.4. p.)). • Koordinuoja el. ryšių, naudojamų valstybės gynybai, saugumui, viešajai tvarkai palaikyti, valstybės sienos apsaugai, laivybos saugumui, jūrų paieškos ir gelbėjimo darbams [...], civilinei aviacijai, traukinių eismo saugumui, stabiliam ir patikimam energetikos sistemos darbui užtikrinti (LRV 2010-10-13 Nr. 1480 (8.5.5. p.)). • Atstovauja Lietuvos interesams [...] palydovų infrastruktūros [...] saugumo užtikrinimu (LRV 2010-10-13 Nr. 1480 (8.5.8. p.)). • Paskelbus karo ar nepaprastąją padėtį [...] ar kitais atvejais [...] reguliuoja el. ryšių veiklą (LRV 2010-10-13 Nr. 1480 (9.6. p.)).
Finansų valdymas	KAM	Kiti teisės aktai: • Pagal kompetenciją planuoja kibernetiniam saugumui užtikrinti reikalingas lėšas (KAM 2014-10-31 Nr. V-1036 (9.7 p.)).
	VRM	• Renka ir analizuoja informaciją apie institucijų valdomų valstybės informacinių išteklių saugą (el. informacijos saugą (kibernetinio saugumo)) ir tam naudojamas lėšas, teikia Vyriausybei ir institucijoms pasiūlymus lėšų šios informacijos saugai poreikio ir efektyvesnio (veiksmingesnio) jų naudojimo (LRS 2011-12-15 Nr. XI-1807 (5 str. 4 d. 2 p.)) (LRV 2001-03-14 Nr. 291 (14.9 p.)). • Teikia pasiūlymus [...] dėl [...] saugos srities projektų poreikio ir efektyvaus ir veiksmingo šių projektų įgyvendinimo, koordinuoja ministerijos kompetencijai priskirtų [...] saugos projektų įgyvendinimą (VRM 2015-06-30 Nr. 1V-534 (4.2.10. ir 4.2.11. p.)).
	SM	• Rengia informacinės visuomenės plėtros srities [...] planavimo dokumentus, koordinuoja jų ir Lietuvos informacinės visuomenės plėtros programos įgyvendinimą; atlieka ES struktūrinių [...] fondų lėšų tarpinės institucijos funkcijas (Informacinės visuomenės plėtros 2014–2020 metų programos „Lietuvos Respublikos skaitmeninė darbotvarkė“ uždavinys – užtikrinti ypač didelės svarbos informacinės infrastruktūros ir valstybės informacinių išteklių apsaugą; 2014-2020 m. ES fondų investicijų veiksmų programos 2 prioriteto „Informacinės visuomenės skatinimas“ priemonė „IRT infrastruktūros optimizavimas ir sauga“) (LRV 2010-10-13 Nr. 1480 (8.6.2. ir 9.14. p.)).
	IVPK	• Planuoja lėšų paskirstymą valstybės informacinių išteklių plėtrai; [...] 2007–2013 m. ES struktūrinės paramos

		[...] planuoja Ekonomikos augimo veiksmų programos 3 prioriteto „Informacinė visuomenė visiems" priemonių [...] įgyvendinimą („Informacinių technologijų sauga"); teikia metodinę pagalbą ir konsultacijas 2014–2020 m. ES struktūrinių fondų investicijų veiksmų programą administruojančioms institucijoms dėl šios veiksmų programos prioriteto „Informacinės visuomenės skatinimas" įgyvendinimo dokumentų rengimo [...] projektų vertinimo, atrankos ir administravimo; dalyvauja koordinuojant valstybės el. ryšių srities investicijų programų rengimą, vertinant šias programas ekonominiu, finansiniu ir techniniu požiūriu, kontroliuojant kaip jos įgyvendinamos (LRS 2011-12-15 Nr. XI-1807 (6 str. 2 d. 3 p.)) (SM 2010-06-23 Nr. 3-401 (10.1.5., 10.1.5.[1]., 10.1.6., 10.2.5. p.)).
Kritinė infrastruktūra	VRM	KSĮ (LRS 2014-12-11 Nr. XII-1428): • Rengia ir teikia Vyriausybei tvirtinti Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką [...] valdytojų sąrašą (7 str. 1 p.). Kiti teisės aktai ir praktinė veikla: • Nustato [...] valstybės informacinių išteklių klasifikavimo pagal juose apdorojamos informacijos svarbą kriterijus ir jų priskyrimo atitinkamai kategorijai tvarką (LRS 2011-12-15 Nr. XI-1807 (4 str. 8 p.)).
	KAM	• Nustatė valstybės gynybos institucijų ypatingos svarbos informacinės infrastruktūros objektus (praktinė veikla).
	RRT	• Nustatė kritinius interneto tinklo ir e. paslaugų elementus (infrastruktūrą) (LRV 2008-07-09 Nr. 678 (8.43 p.)) (praktinė veikla).
	LRS	• Nustato strateginę ar svarbią reikšmę nacionaliniam saugumui turinčias įmones ir įrenginius (LRS 2002-10-10 Nr. IX-1132 (3 str., 4 str., 5 str.)).
		Persidengia įstaigų, atsakingų už kibernetinio saugumo ir el. informacijos saugos sričių valdymą, koordinavimą, priemonių nustatymą, vykdomos funkcijos
Reglamentavimas	KAM	KSĮ (LRS 2014-12-11 Nr. XII-1428): • Rengia ir teikia Vyriausybei tvirtinti organizacinius ir techninius kibernetinio saugumo reikalavimus (6 str. 1 p.). • Teikia Vyriausybei tvirtinti tipinius kibernetinių incidentų valdymo [...] planus; tvirtina [...] kibernetinės gynybos planus (6 str. 4 p.).
	KS Taryba	• Teikia kibernetinio saugumo dalyviams rekomendacijas dėl kibernetinio saugumo stiprinimo (9 str. 4 d. 4 p.)).
	NKSC	• Teikia konsultacijas ir rekomendacijas [...] kibernetinio saugumo klausimais, teikia [...] rekomendacijas dėl kibernetinio saugumo stiprinimo (10 str. 2 d. 4 p.). • Vykdo informacijos sklaidą kibernetinio saugumo klausimais (10 str. 2 d. 9 p.), skelbia [...] metodinę informaciją, rekomendacijas ir kitą su kibernetiniu saugumo užtikrinimu susijusią [...] informaciją (10 str. 4 d. 1 p.). • Kartu su verslo subjektais, mokslo ir studijų institucijomis ir kitais kibernetinio saugumo dalyviais plėtoja bendrus kibernetinio saugumo projektus (10 str. 3 d. 9 p.). • Duoda [...] nurodymus, susijusius su kibernetinio saugumo užtikrinimu [...] taiko [..] kibernetinio saugumo užtikrinimo priemones (10 str. 3 d. 4 p.).
	PD	• Nustato [...] informacijos, reikalingos kibernetiniams incidentams [...] užkardyti ir tirti, pateikimo tvarką (12 str. 2 p.). • Duoda [...] nurodymus [...] apriboti [...] paslaugų teikimą paslaugų gavėjui [...] taikyti priemones [...] išsaugoti informaciją [...] gauna paslaugų naudotojo srauto duomenis ir kontroliuoja perduodamos informacijos turinį (12 str. 3 p., 4 p.).
	VDAI	• Nustato [...] informacijos apie kibernetinius incidentus [...] ir taikytas šių incidentų valdymo priemones pateikimo tvarką (11 str. 3 p.).
	RRT	• Rengia ir tvirtina organizacinius ir techninius reikalavimus, taikomus el. informacijos prieglobos paslaugų saugumui ir vientisumui užtikrinti (8 str. 1 d. 2 p.). • Rengia ir tvirtina informacijos apie kibernetinius incidentus ir taikytas šių incidentų valdymo priemones teikimo RRT tvarką ir sąlygas (8 str. 1 d. 1 p.), techninės informacijos [...] teikimo RRT tvarką (8 str. 1 d. 3 p.). • Duoda privalomus nurodymus [...] ryšių paslaugų tiekėjams (8 str. 2 d.).
	CERT	Kiti teisės aktai ir praktinė veikla: • Rengia rekomendacijas apie grėsmes, organizuoja seminarus, mokymus, konsultacijas, rengia rekomendacijas teikėjams, CERT padaliniams ir paslaugų gavėjams apie apsaugą nuo incidentų (LRV 2008-07-09 Nr. 678 (8.43 p.)) (praktinė veikla). • Teikia pasiūlymus dėl teisės aktų, susijusių su el. ryšių tinklų ir informacijos saugumu (LRV 2008-07-09 Nr. 678 (8.43 p.)) (praktinė veikla).
	VRM	• Rengia informacijos saugos reikalavimus, saugos dokumentų turinio gaires; derina [...] su informacijos sauga susijusių teisės aktų, saugos dokumentų projektus [...] projektų nuostatas, susijusias su informacijos sauga (LRS 2011-12-15 Nr. XI-1807 (5 str. 4 d. 3 p., 5 p., 6 p.)). • Nustato informacijos svarbos įvertinimo [...] klasifikavimo [...] pagal apdorojamos informacijos svarbą kriterijus ir [...] priskyrimo atitinkamai kategorijai tvarką (LRS 2011-12-15 Nr. XI-1807 (5 str. 4 d. 8 p.)). • Konsultuoja [...] valstybės informacinių išteklių saugos klausimais (LRS 2011-12-15 Nr. XI-1807 (5 str. 4 d. 7 p.)).
	SM	• Rengia ir teikia pasiūlymus Vyriausybei dėl [...] rekomenduotinų taikyti techninių reikalavimų (standartų) (LRS 2011-12-15 Nr. XI-1807 (5 str. 2 d. 1 p.)). • [...] duoda [...] privalomus nurodymus, užduotis ir užsakymus apsaugoti ir palaikyti reikiamus el. ryšių tinklus, taip pat juos sujungti ir prireikus apriboti visuomenės galimybę naudotis el. ryšių tinklais nenugalimos jėgos ir ekstremalių situacijų ar kitų ypatingų aplinkybių atvejais, taip pat siekdama pasirengti visuotinei mobilizacijai, valstybės gynybai, užtikrinti valstybės saugumą ir viešąją tvarką (LRV 2010-10-13 Nr. 1480 (8.5.6. p.)). • [...] nustato viešųjų ryšių tinklų ir viešųjų el. ryšių paslaugų palaikymo prioritetus tinklo katastrofinio gedimo ar nenugalimos jėgos pasireiškimo, taip pat ekstremalių situacijų ir kitais ypatingų aplinkybių atvejais, kad

		būtų palaikomas aukščiausias paslaugų lygis (LRV 2010-10-13 Nr. 1480 (8.5.7. p.)).
	IVPK	• Konsultuoja [...] techninės ir programinės įrangos priežiūros [...] klausimais; rengia metodinius dokumentus informacinių technologijų paslaugų valdymo [...] klausimais (sutrikimų/incidentų, problemų, keitimų, sąrankos valdymas (LRS 2011-12-15 Nr. XI-1807 (6 str. 2 d. 10 p.) (SM 2010-06-23 Nr. 3-401 (10.2.12. p.)).
	Kitos ministerijos	• Suderinusios su VRM ir Valstybės saugumo departamentu tvirtina jų ministrų valdymo sritims priskirtų strateginę ar svarbią reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių informacinės saugos reikalavimus (LRV 2004-06-08 Nr. 699).
Analizė ir stebėsena	KS Taryba	KSĮ (LRS 2014-12-11 Nr. XII-1428): • Analizuoja kibernetinio saugumo užtikrinimo tobulinimo tendencijas (9 str. 4 d. 3 p.).
	NKSC	• Atlieka [...] atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams stebėseną (10 str. 2 d. 2 p.). • Analizuoja nacionalinę kibernetinio saugumo situaciją ir rengia nacionalinio kibernetinio saugumo būklės ataskaitas (10 str. 2 d. 5 p.). • Susipažįsta su [...] audito išvadomis [...], rizikos analizėmis (10 str. 3 d. 2 p.). • Valdo kibernetinio saugumo informacinį tinklą (rekomendacijos, nurodymai, techniniai sprendimai, kontaktinė informacija ir kt.) (10 str. 2 d. 8 p.).
	PD	• Renka, analizuoja ir apibendrina informaciją apie kibernetinius incidentus (12 str. 1 p.).
	VDAI	• Renka, analizuoja ir vertina informaciją apie kibernetinius incidentus [...] ir taikytas šių incidentų valdymo priemones (11 str. 4 p.). • Teikia [...] informaciją apie kibernetinio saugumo [...] rizikos veiksnius, pavojus ir grėsmes kibernetinėje erdvėje (11 str. 2 p.).
	RRT	• Atlieka [...] interneto prieigos tinklų infrastruktūros vientisumo tyrimus (8 str. 1 d. 4 p.). • Atlieka [...] el. informacijos prieglobos paslaugų kibernetinio saugumo būsenos tyrimus (8 str. 1 d. 5 p.).
	CERT	Kiti teisės aktai ir praktinė veikla: • Vykdo el. ryšių tinklų ir informacijos saugumo būsenos stebėseną Lietuvoje (LRV 2008-07-09 Nr. 678 (8.43 p.)) (praktinė veikla).
	KAM	• Analizuoja kibernetinio saugumo ir gynybos vystymosi tendencijas Lietuvoje ir pasaulyje, vertina užsienio šalių patirtį ir siūlymus (KAM 2014-10-31 Nr. V-1036 (9.4 p.)).
	VRM	• Renka ir analizuoja informaciją apie [...] saugą [...] teikia Vyriausybei ir institucijoms siūlymus dėl [...] saugos. (LRS 2011-12-15 Nr. XI-1807 (5 str. 4 d. 2 p.)). • Atlieka saugos reikalavimų laikymosi priežiūrą tiek, kiek tai neapima kibernetinio saugumo (LRS 2011-12-15 Nr. XI-1807 (5 str. 4 d. 4 p.)). • Organizuoja informacinių technologijų priemonių valdymo ir saugos vertinimą (LRS 2011-12-15 Nr. XI-1807 (5 str. 4 d. 1 p.)) (LRV 2001-03-14 Nr. 291 (14.8 p.)). • Atlieka [...] el. informacijos saugos reikalavimų stebėseną (LRS 2011-12-15 Nr. XI-1807 (43.[1] str. 1 d.)). • Nustato grėsmių ir pažeidžiamumų vertinimo metodiką ir vykdo šios srities vertinimus (LRV 2011-06-29 Nr. 796 (priedas 5 p.)) (LRV 2014-10-03 Nr. 1094 (5.3.5. p.)). • Renka ir sudaro kontaktinių asmenų, atsakingų už reagavimą į el. informacijos saugos incidentus sąrašą (MP 2011-10-19 Nr. 263 DG 2012-01-13 protokolo Nr. LV-9 1.5 p.) (praktinė veikla).
	PAGD	• Koordinuoja Lietuvos nacionalinės rizikos analizės atlikimą (kibernetinės atakos) (VRM 2010-12-31 Nr.1V-831 (9.1. ir 10.1.2. p.)).
	SM	• Renka, kaupia, sistemina ir analizuoja informaciją, susijusią su susisiekimo ministrui pavestomis valdymo sritimis; analizuoja kitų valstybių patirtį, susijusią su susisiekimo ministrui pavestomis valdymo sritimis (el. ryšiai, informacinės visuomenės plėtra) (LRV 2010-10-13 Nr. 1480 (9.21. p.)).
	IVPK	• Renka ir analizuoja informaciją apie informacinių technologijų plėtros planų įgyvendinimą (LRS 2011-12-15 Nr. XI-1807 (6 str. 2 d. 6 p.)). • Kaupia, sistemina ir apibendrina informaciją apie programinės įrangos naudojimą [...] ir jos poreikį (SM 2010-06-23 Nr. 3-401 (10.2.17 p.)).
	Žvalgybos institucijos	• Renka informaciją apie rizikos veiksnius, pavojus ir grėsmes [...] teikia [...] metinį rizikos veiksnių, pavojų ir grėsmių [...] vertinimą ir ataskaitą [...] grėsmių [...] vertinimus pagal savo veiklos sritis (LRS 2012-10-17 Nr. XI-2289 (8 str., 22 str. 3 d.)).
Incidentų valdymas	NKSC	KSĮ (LRS 2014-12-11 Nr. XII-1428): • Reaguoja į kibernetinius incidentus [..], (10 str. 2 d. 2 p.). • Taiko technines priemones, siekdamas įvertinti [...] infrastruktūrų atsparumą kibernetiniams incidentams (10 str. 3 d. 3 p.).
	KS Taryba	• Teikia [...] išvadas ir pasiūlymus dėl kibernetinių incidentų valdymo (9 str. 4 d. 3 p.)).
	VDAI	• Atlieka [...] patikrinimus, kai [...] kibernetiniai incidentai gali turėti įtakos asmens duomenų apsaugai (11 str. 1 p.). • Tikrina [...] ir priima sprendimus dėl asmens duomenų tvarkymo pažeidimų kibernetinėje erdvėje (11 str. 5 p.).
	PD	• Vykdo kibernetinių incidentų, galimai turinčių nusikalstamos veikos požymių tyrimus (12 str.).
	NKSC	Kiti teisės aktai ir praktinė veikla: • vykdo kibernetinių incidentų valdymo padalinio veiklą (CERT, koordinuoja kibernetinių incidentų valdymą) (KAM 2014-12-29 Nr. V-1321 (10.1 p.)) (praktinė veikla).
	CERT	• Atlieka el. ryšių tinklų ir informacijos saugumo incidentų tyrimus ir padalinio veiklą (CERT), veiksmų koordinavimą sprendžiant incidentus (nacionalinis CERT) (LRV 2008-07-09 Nr. 678 (8.43 p.)) (praktinė veikla). • Skelbia įvykusių incidentų statistiką, įspėjimus apie galimas incidentų grėsmes (LRV 2008-07-09 Nr. 678 (8.43 p.)) (praktinė veikla).

	Nevykdomos arba netinkamai vykdomos priskirtos funkcijos kibernetinio saugumo ir el. informacijos saugos srityse	
VRM	KSĮ (LRS 2014-12-11 Nr. XII-1428): • Rengia ir teikia Vyriausybei tvirtinti Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką [...] valdytojų sąrašą (7 str. 1 p.).	Kiti teisės aktai: • Renka ir analizuoja informaciją apie institucijų ir įstaigų valdomų valstybės informacinių išteklių saugą (el. informacijos saugą (kibernetinio saugumo)) ir tam naudojamas lėšas, teikia Vyriausybei ir institucijoms pasiūlymus lėšų šios informacijos saugai poreikio ir efektyvesnio (veiksmingesnio) jų naudojimo (LRS 2011-12-15 Nr. XI-1807 (5 str. 4 d. 2 p.)) (LRV 2001-03-14 Nr. 291 (14.9 p.)). • Teikia pasiūlymus [...] dėl [...] saugos srities projektų poreikio ir efektyvaus ir veiksmingo šių projektų įgyvendinimo; koordinuoja ministerijos kompetencijai priskirtų [...] saugos projektų įgyvendinimą (VRM 2015-06-30 Nr. 1V-534 (4.2.10. ir 4.2.11. p.)). • Rengia[...] grėsmių ir pažeidžiamumų vertinimo metodiką (LRV 2011-06-29 Nr. 796 (priedas 5 p.)) (LRV 2014-10-03 Nr. 1094 (5.3.5. p.).

Šaltinis – Valstybės kontrolė.