Suvestinė redakcija nuo 2022-02-04

Įsakymas paskelbtas: TAR 2020-07-21, i. k. 2020-16183

LIETUVOS RESPUBLIKOS EKONOMIKOS IR INOVACIJŲ MINISTRAS

ĮSAKYMAS DĖL LICENCIJŲ INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2020 m. liepos 21 d. Nr. 4-586
Vilnius

Įgyvendindamas Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Bendrųjų reikalavimų aprašas), 7.1 papunktį, 11, 19, 26 punktus, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, 6 punktą:

1. T v i r t i n u Licencijų informacinės sistemos duomenų saugos nuostatus (pridedama).

2. P a v e d u Licencijų informacinės sistemos (toliau – LIS) tvarkytojui:

2.1. paskirti LIS saugos įgaliotinį (įgaliotinius) ir LIS administratorių (administratorius);

2.2. per 5 mėnesius nuo šio įsakymo įsigaliojimo dienos parengti, suderinti ir pateikti Lietuvos Respublikos ekonomikos ir inovacijų ministerijai tvirtinti LIS elektroninės informacijos saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentų, nurodytų Bendrųjų reikalavimų aprašo 7.2, 7.3 ir 7.4 papunkčiuose, projektus.

Ekonomikos ir inovacijų ministras Rimantas Sinkevičius

SUDERINTA
Nacionalinio kibernetinio saugumo centro

prie Krašto apsaugos ministerijos
2020-07-14 raštu Nr. (4.1E)6K-443

PATVIRTINTA
Lietuvos Respublikos ekonomikos ir
inovacijų ministro
2020 m. liepos 21 d. įsakymu Nr. 4-586

LICENCIJŲ INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Licencijų informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reguliuoja Licencijų informacinės sistemos (toliau – LIS) elektroninės informacijos saugos ir kibernetinio saugumo politiką. Saugos nuostatų turinį nustato Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 30 straipsnio 3 dalis.

2. Saugos nuostatuose vartojamos sąvokos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas), ir Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – Techniniai elektroninės informacijos saugos reikalavimai).

Punkto pakeitimai:
Nr. 4-175, 2022-02-03, paskelbta TAR 2022-02-03, i. k. 2022-01945

3. Saugos nuostatų, LIS valdytojo patvirtintų Licencijų informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių, Licencijų informacinės sistemos veiklos tęstinumo valdymo plano, Licencijų informacinės sistemos naudotojų administravimo taisyklių (toliau visi kartu – Saugos dokumentai) taikymas ir naudojimas:

3.1. Saugos dokumentai taikomi:

3.1.1. LIS valdytojui – Lietuvos Respublikos ekonomikos ir inovacijų ministerijai (Gedimino pr. 38, 01104 Vilnius);

3.1.2. LIS tvarkytojui – valstybės įmonei Registrų centrui (Lvovo g. 25-101, 09320 Vilnius);

3.1.3. LIS saugos įgaliotiniui, LIS administratoriams, LIS naudotojams, LIS funkcionuoti reikalingų paslaugų teikėjams.

4. Saugos nuostatai yra vieši ir skelbiami Lietuvos Respublikos teisės aktų registre. Licencijų informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės, Licencijų informacinės sistemos veiklos tęstinumo valdymo planas, Licencijų informacinės sistemos naudotojų administravimo taisyklės nėra skelbiami teisės aktų registre. Šių dokumentų teikimas

asmenims yra ribojamas, atsižvelgiant į Lietuvos Respublikos informacinių išteklių valdymo įstatymo 43 straipsnio 1 ir 7 dalis ir Lietuvos Respublikos teisės gauti informaciją iš valstybės ir savivaldybės institucijų ir įstaigų įstatymo 2 straipsnio 2 dalies 3 punktą – LIS naudotojams, LIS funkcionuoti reikalingų paslaugų teikėjams, tretiesiems asmenims suteikiama teisė susipažinti tik su jų santrauka, vadovaujantis būtinumo žinoti principu, kuris reiškia, kad suteikiama tik tokia informacija, kuri reikalinga tiesioginei veiklai vykdyti, Saugos nuostatų V skyriuje nustatyta tvarka.

5. Saugos dokumentų santrauka rengiama vadovaujantis būtinumo žinoti principu, apibrėžtu Saugos nuostatų 4 punkte. Saugos dokumentus tvirtina LIS valdytojas LIS tvarkytojo teikimu.

6. Elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo prioritetinės kryptys:

6.1. elektroninės informacijos saugos – elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo – užtikrinimas;

6.2. LIS kibernetinio saugumo užtikrinimas;

6.3. asmens duomenų apsauga;

6.4. LIS naudotojų mokymas.

7. Elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo tikslai:

7.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti LIS elektroninę informaciją;

7.2. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

7.3. vykdyti elektroninės informacijos saugos (kibernetinių) incidentų asmens duomenų saugumo pažeidimų prevenciją, reaguoti į elektroninės informacijos saugos (kibernetinius) incidentus, asmens duomenų saugumo pažeidimus ir juos operatyviai suvaldyti.

8. LIS valdytojo funkcijos:

8.1. atlikti LIS nuostatuose nustatytas funkcijas;

8.2. tvirtinti Saugos dokumentus ir kitus teisės aktus, susijusius su LIS elektroninės informacijos sauga ir kibernetiniu saugumu;

8.3. koordinuoti LIS tvarkytojo darbą įgyvendinant elektroninės informacijos saugos ir kibernetinio saugumo reikalavimus;

8.4. nagrinėti LIS tvarkytojo pasiūlymus dėl LIS elektroninės informacijos saugos ir kibernetinio saugumo tobulinimo ir priimti dėl jų sprendimus;

8.5. skirti LIS saugos įgaliotinį ir LIS administratorių arba pavesti juos skirti LIS tvarkytojui;

8.6. atlikti kitas Saugos nuostatuose ir Saugos nuostatų 21 punkte nurodytuose teisės aktuose nustatytas LIS valdytojo funkcijas.

9. LIS tvarkytojo funkcijos:

9.1. atlikti LIS nuostatuose nustatytas funkcijas;

9.2. užtikrinti tinkamą saugos dokumentų ir kitų LIS valdytojo priimtų teisės aktų, susijusių su LIS elektroninės informacijos sauga ir kibernetiniu saugumu, įgyvendinimą;

9.3. prižiūrėti LIS komponentus (kompiuterius, operacines sistemas ir kitus LIS komponentus, nurodytus Saugos nuostatų 16.3 papunktyje), užtikrinti jų veikimą;

9.4. įgyvendinti LIS elektroninės informacijos saugos ir kibernetinio saugumo reikalavimus;

9.5. užtikrinti LIS elektroninės informacijos saugą ir kibernetinį saugumą;

9.6. teikti LIS valdytojui pasiūlymus dėl LIS elektroninės informacijos saugos ir kibernetinio saugumo tobulinimo;

9.7. LIS valdytojo pavedimu skirti LIS saugos įgaliotinį ir LIS administratorių;

9.8. atlikti kitas Saugos nuostatuose ir Saugos nuostatų 21 punkte nurodytuose teisės aktuose nustatytas LIS tvarkytojo funkcijas.

10. Už elektroninės informacijos saugą ir kibernetinį saugumą pagal kompetenciją atsako LIS valdytojas ir LIS tvarkytojas.

11. LIS valdytojas atsako už elektroninės informacijos saugos ir kibernetinio saugumo politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą.

12. LIS tvarkytojas atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos dokumentuose nustatyta tvarka.

13. LIS saugos įgaliotinio funkcijos:

13.1. koordinuoti ir prižiūrėti elektroninės informacijos saugos ir kibernetinio saugumo politikos įgyvendinimą Saugos dokumentuose nustatyta tvarka;

13.2. atlikti Saugos dokumentuose ir Bendrųjų elektroninės informacijos saugos reikalavimų apraše nustatytas funkcijas;

13.3. atlikti Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas), nustatytas už kibernetinio saugumo organizavimą ir užtikrinimą atsakingo asmens funkcijas.

14. Saugos įgaliotinis ir LIS administratorius gali būti skiriami keliems LIS posistemiams, funkciškai savarankiškoms sudedamosioms dalims ar tam tikroms saugos įgaliotinio ir LIS administratoriaus funkcijoms atlikti, tačiau turi būti užtikrintas tinkamas saugos įgaliotinio ir LIS administratoriaus funkcijų atlikimas. Jeigu skiriami atskiro LIS posistemio saugos įgaliotiniai ir LIS administratoriai funkciškai savarankiškoms sudedamosioms dalims ar tam tikroms saugos įgaliotinio ir administratoriaus funkcijoms atlikti, turi būti aiškiai nurodyta, kokiam LIS posistemiui, funkciškai savarankiškoms sudedamosioms dalims ar kurioms saugos įgaliotinio ir administratoriaus funkcijoms atlikti skiriamas konkretus saugos įgaliotinis ir administratorius, taip pat vienam iš saugos įgaliotinių ir administratorių pavedama koordinuoti šių saugos įgaliotinių ir administratorių veiklą.

15. Saugos įgaliotinis negali atlikti LIS administratoriaus funkcijų.

16. LIS administratoriai pagal atliekamas funkcijas skirstomi į šias grupes:

16.1. koordinuojantysis administratorius, kuris prižiūri LIS administratorių veiklą, siekdamas užtikrinti tinkamą LIS administratorių funkcijų atlikimą;

16.2. LIS naudotojų administratoriai, kurie atlieka funkcijas, susijusias su LIS naudotojų teisių valdymu;

16.3. LIS komponentų administratoriai, kurie atlieka funkcijas, susijusias su LIS komponentais (kompiuteriais, operacinėmis sistemomis, duomenų bazėmis ir jų valdymo sistemomis, taikomųjų programų sistemomis, užkardomis, įsilaužimų aptikimo ir prevencijos sistemomis, elektroninės informacijos perdavimo tinklais, duomenų saugyklomis, bylų serveriais ir kita technine ir programine įranga, kurios pagrindu funkcionuoja LIS ir užtikrinama joje tvarkomos elektroninės informacijos sauga ir kibernetinis saugumas), bei LIS komponentų sąranka;

16.4. LIS administratoriai, kurie atlieka funkcijas, susijusias su informacinių sistemų pažeidžiamų vietų nustatymu, saugumo reikalavimų atitikties nustatymu ir stebėsena.

17. LIS administratoriai yra atsakingi už tinkamą saugos dokumentuose nustatytų funkcijų atlikimą.

18. LIS administratoriai privalo vykdyti visus saugos įgaliotinio nurodymus ir pavedimus dėl LIS saugos ir kibernetinio saugumo užtikrinimo, pagal kompetenciją reaguoti į elektroninės informacijos saugos ir kibernetinius incidentus ir nuolat teikti saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę.

19. Atlikdami LIS sąrankos pakeitimus, LIS komponentų administratoriai turi laikytis Licencijų informacinės sistemos pokyčių valdymo tvarkos, nustatytos LIS valdytojo tvirtinamose Licencijų informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse.

20. LIS komponentų administratoriai LIS sąranką ir LIS būsenos rodiklius privalo patikrinti (peržiūrėti) reguliariai – ne rečiau kaip kartą per metus ir (arba) po LIS pokyčio.

21. Tvarkant LIS elektroninę informaciją ir užtikrinant jos saugą, vadovaujamasi šiais teisės aktais:

21.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);

21.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

21.3. Lietuvos Respublikos kibernetinio saugumo įstatymu;

21.4. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

21.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu;

21.6. Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Klasifikavimo gairių aprašas);

21.7. Lietuvos standartais LST EN ISO/IEC 27002 ir LST EN ISO/IEC 27001;

21.8. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu;

21.9. Techniniais elektroninės informacijos saugos reikalavimais.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

22. LIS tvarkoma elektroninė informacija priskiriama svarbios elektroninės informacijos kategorijai. Elektroninė informacija šiai kategorijai priskiriama vadovaujantis Klasifikavimo gairių aprašo 8.1 ir 8.2 papunkčiais.

23. Informacinė sistema pagal joje tvarkomos elektroninės informacijos svarbą, vadovaujantis Klasifikavimo gairių aprašo 12.2 papunkčiu, priskiriama antrajai kategorijai.

24. Rizikos vertinimo organizavimas:

24.1. LIS saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius grupės „Informacijos technologija. Saugumo technika“ standartus, kasmet arba

įvykus esminių organizacinių ar sisteminių pokyčių organizuoja LIS rizikos įvertinimą. LIS rizikos vertinimas gali būti atliekamas kartu su informacinių technologijų saugos atitikties vertinimu.

24.2. Prireikus saugos įgaliotinis gali organizuoti neeilinį LIS rizikos įvertinimą. LIS tvarkytojo rašytiniu pavedimu LIS rizikos įvertinimą gali atlikti pats saugos įgaliotinis. Organizuojant rizikos vertinimą, rekomenduojama LIS rizikos vertinimą įtraukti į LIS tvarkytojo veiklos rizikos vertinimo procesus.

24.3. Organizuojant rizikos vertinimą turi būti paskirtas (-i) už rizikos vertinimą, rizikos vertinimo proceso priežiūrą ir nuolatinį tobulinimą atsakingas (-i) asmuo (-enys) ir nustatyti jam (jiems) taikomi kvalifikaciniai reikalavimai. Atsakingu asmeniu gali būti skiriamas LIS valdytojo arba LIS tvarkytojo darbuotojas LIS valdytojo ar LIS tvarkytojo įsakymu saugos įgaliotinio teikimu, arba sudaroma sutartis su rizikos vertinimo, rizikos vertinimo proceso priežiūros ir nuolatinio tobulinimo paslaugas teikiančiu subjektu.

24.4. Rizikos vertinimo metu turi būti:

24.4.1. nustatomos grėsmės ir pažeidžiamumas, galintys turėti įtakos LIS elektroninės informacijos saugai ir kibernetiniam saugumui;

24.4.2. nustatomos galimos grėsmių ir pažeidžiamumo poveikio vykdomai veiklai sritys;

24.4.3. įvertinama LIS pažeidimo grėsmių tikimybė ir pasekmės;

24.4.4. nustatomas rizikos lygis ir įvertinamos identifikuotos grėsmių tikimybės, kurios išdėstomos prioriteto tvarka pagal svarbą, nustatomą atsižvelgiant į atliktą rizikos vertinimą.

24.5. Rizikos veiksniai rizikos įvertinimo ataskaitoje turi būti išdėstyti pagal prioritetus ir priimtiną rizikos lygį. LIS rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama LIS valdytojo vadovui ir LIS tvarkytojo vadovui. Rengiant rizikos įvertinimo ataskaitą, įvertinami rizikos veiksniai, galintys turėti įtakos LIS elektroninės informacijos saugai ir kibernetiniam saugumui, jų galima žala, pasireiškimo tikimybė ir pobūdis, galimi rizikos valdymo būdai, rizikos priimtinumo kriterijai. Svarbiausi rizikos veiksniai yra šie:

24.5.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais triktys, programinės įrangos klaidos, netinkamas veikimas ir kita);

24.5.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

24.5.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

24.6. Atsižvelgdamas į rizikos įvertinimo ataskaitą, LIS valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių, organizacinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

24.7. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas LIS valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai.

24.8. Atsižvelgiant į atlikto rizikos vertinimo rezultatus, taip pat jeigu Saugos nuostatų 25 punkte nustatyta tvarka atliekamo informacinių technologijų saugos atitikties vertinimo metu nustatoma kibernetinių incidentų valdymo ir šalinimo, organizacijos nepertraukiamos veiklos užtikrinimo trūkumų, atitinkamai turi būti tobulinamas LIS veiklos tęstinumo valdymo planas ir (arba) kibernetinių incidentų valdymo planas, patvirtinti LIS valdytojo. Šių planų veiksmingumo išbandymo rezultatai išdėstomi šių planų veiksmingumo išbandymo ir pastebėtų trūkumų ataskaitose, kurių kopijos ne vėliau kaip per 5 darbo dienas nuo šių dokumentų priėmimo pateikiamos Nacionaliniam kibernetinio saugumo centrui.

25. Informacinių technologijų saugos atitikties vertinimo organizavimas:

25.1. siekiant užtikrinti Saugos dokumentuose nustatytų elektroninės informacijos saugos ir kibernetinio saugumo reikalavimų įgyvendinimo organizavimą ir kontrolę, ne rečiau kaip kartą per metus, jei teisės aktuose nenustatyta kitaip, turi būti organizuojamas LIS informacinių technologijų saugos atitikties vertinimas;

25.2. informacinių technologijų saugos atitikties vertinimas atliekamas Informacinių technologijų saugos atitikties vertinimo metodikoje, patvirtintoje Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“, nustatyta tvarka.

Papunkčio pakeitimai:

Nr. 4-175, 2022-02-03, paskelbta TAR 2022-02-03, i. k. 2022-01945

25.3. LIS atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus.

25.4. atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos vertinimo ataskaita, kuri pateikiama LIS valdytojo vadovui ir LIS tvarkytojo vadovui, ir pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus skiria ir įgyvendinimo terminus nustato LIS valdytojo vadovas.

25.5. informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas LIS valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai.

26. Elektroninės informacijos saugos ir kibernetinio saugumo būklės gerinimas:

26.1. Techninės, programinės, organizacinės ir kitos LIS elektroninės informacijos saugos ir kibernetinio saugumo priemonės pasirenkamos atsižvelgiant į LIS valdytojo turimus išteklius, vadovaujantis šiais principais:

26.1.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

26.1.2. priemonės diegimo kaina turi būti tapati tvarkomos elektroninės informacijos vertei;

26.2. Atsižvelgiant į priemonių efektyvumą ir taikymo tikslingumą, turi būti įdiegtos prevencinės, detekcinės ir korekcinės elektroninės informacijos saugos ir kibernetinio saugumo priemonės.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

27. Organizaciniai ir techniniai elektroninės informacijos saugos ir kibernetinio saugumo reikalavimai nustatomi pagal Saugos nuostatų 22–23 punktuose nustatytą LIS svarbos kategoriją, vadovaujantis Saugos nuostatų 21 punkte nurodytais teisės aktais ir standartais.

28. Kibernetinio saugumo priemonės, nurodytos Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo priede, turi būti diegiamos atsižvelgiant į naujausius technologinius sprendimus, vadovaujantis gamintojo pateikiama bent viena gerosios saugumo praktikos rekomendacija.

29. Organizacinių ir techninių elektroninės informacijos saugos ir kibernetinio saugumo priemonių užtikrinimas turi būti grindžiamas grėsmių ir pažeidžiamumo, galinčio turėti įtakos LIS elektroninės informacijos saugai ir kibernetiniam saugumui, rizikos vertinimu, atsižvelgiant į naujausius technikos laimėjimus.

30. Programinės įrangos, skirtos LIS apsaugoti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.), naudojimo nuostatos ir jos atnaujinimo reikalavimai:

30.1. Tarnybinėse stotyse ir vidinių LIS naudotojų kompiuteriuose turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingos programinės įrangos aptikimo, stebėjimo realiu laiku priemonės.

30.2. LIS komponentai be kenksmingos programinės įrangos aptikimo priemonių gali būti eksploatuojami, jeigu rizikos vertinimo metu patvirtinama, kad šių komponentų rizika yra priimtina.

30.3. Kenksmingos programinės įrangos aptikimo priemonės turi atsinaujinti automatiškai, ne rečiau kaip kartą per 24 valandas. LIS komponentų administratorius turi būti automatiškai informuojamas elektroniniu paštu apie tai, kuriems LIS posistemiams, funkciškai savarankiškoms sudedamosioms dalims, vidinių LIS naudotojų kompiuteriams ir kitiems LIS komponentams yra pradelstas kenksmingos programinės įrangos aptikimo priemonių atsinaujinimo laikas, taip pat jei kenksmingos programinės įrangos aptikimo priemonės netinkamai veikia arba yra išjungtos.

31. Programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos:

31.1. LIS tarnybinėse stotyse ir vidinių LIS naudotojų kompiuteriuose turi būti naudojama tik legali programinė įranga.

31.2. Vidinių LIS naudotojų kompiuteriuose naudojama programinė įranga turi būti įtraukta į su LIS valdytoju suderintą leistinos naudoti programinės įrangos sąrašą. Leistinos programinės įrangos sąrašą turi parengti, ne rečiau kaip kartą per metus peržiūrėti ir prireikus atnaujinti saugos įgaliotinis.

31.3. Tarnybinių stočių ir vidinių LIS naudotojų kompiuterių operacinės sistemos, kibernetiniam saugumui užtikrinti naudojamų priemonių ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai, klaidų pataisymai turi būti operatyviai išbandomi ir įdiegiami.

31.4. Saugos administratorius reguliariai, ne rečiau kaip kartą per savaitę, turi įvertinti informaciją apie neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumo svarbos lygius LIS posistemiuose, funkciškai savarankiškose sudedamosiose dalyse, vidinių LIS naudotojų kompiuteriuose. Apie įvertinimo rezultatus saugos administratorius turi informuoti saugos įgaliotinį ir kibernetinio saugumo vadovą.

31.5. Programinė įranga turi būti prižiūrima ir atnaujinama laikantis gamintojo reikalavimų ir rekomendacijų.

31.6. Programinės įrangos diegimą, konfigūravimą, priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai – LIS komponentų administratoriai arba tokias paslaugas teikiantys kvalifikuoti paslaugų teikėjai.

31.7. Programinė įranga turi būti testuojama naudojant atskirą testavimo aplinką, kurioje esantys asmens duomenys turi būti naudojami vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu.

31.8. LIS programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS*), dedikuoto atkirtimo nuo paslaugos (angl. *DDOS*) ir kitų; pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. *The Open Web Application Security Project (OWASP)*) interneto svetainėje www.owasp.org.

32. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių ir kt.) pagrindinės naudojimo nuostatos:

32.1. Kompiuterių tinklai turi būti atskirti nuo viešųjų elektroninių ryšių tinklų (interneto) naudojant užkardas, automatinę įsilaužimų aptikimo ir prevencijos įrangą, atkirtimo nuo paslaugos, dedikuoto atkirtimo nuo paslaugos įrangą.

32.2. Kompiuterių tinklų perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešuose ryšių tinkluose naršančių vidinių LIS naudotojų kompiuterinę įrangą nuo kenksmingo kodo. Visas duomenų srautas į internetą ir iš jo turi būti filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos.

32.3. Apsaugai nuo elektroninės informacijos nutekinimo turi būti naudojama duomenų srautų analizės ir kontrolės įranga.

32.4. Turi būti naudojamos turinio filtravimo sistemos.

32.5. Turi būti naudojamos taikomųjų programų kontrolės sistemos.

33. Užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą, turi būti naudojamas šifravimas, virtualus privatusis tinklas, skirtinės linijos, saugus elektroninių ryšių tinklas ar kitos priemonės, kuriomis užtikrinamas saugus elektroninės informacijos perdavimas. Metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą (nuotolinio prisijungimo prie LIS būdai, protokolai, elektroninės informacijos keitimosi formatai, šifravimo, elektroninės informacijos kopijų skaičiaus reikalavimai, reikalavimai teikti ir (ar) gauti elektroninę informaciją automatiniu būdu tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas ir panašiai), nustatyti Licencijų informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse.

34. Stacionariuosius kompiuterius leidžiama naudoti tik LIS valdytojo ir LIS tvarkytojų patalpose. Nešiojamiesiems kompiuteriams, išnešamiems iš LIS valdytojo ar LIS tvarkytojo patalpų, turi būti taikomos papildomos saugos priemonės (elektroninės informacijos šifravimas, prisijungimo ribojimas ir panašiai).

35. Pagrindiniai organizaciniai ir techniniai elektroninės informacijos saugos ir kibernetinio saugumo reikalavimai:

35.1. organizaciniai ir techniniai elektroninės informacijos saugos ir kibernetinio saugumo reikalavimai detalizuojami informacinės sistemos ir kibernetinio saugumo politiką įgyvendinančiuose dokumentuose;

35.2. turi būti naudojama ir operatyviai atnaujinama programinė įranga, skirta apsaugoti LIS nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir pan.). Išsamios šios programinės įrangos naudojimo

nuostatos ir jos atnaujinimo reikalavimai (ilgiausias leidžiamas neatnaujinimo laikas ir kt.) nustatomi LIS saugaus elektroninės informacijos tvarkymo taisyklėse;

35.3. LIS techninėje įrangoje ir LIS naudotojų kompiuteriuose turi būti naudojama tik legali programinė įranga. Išsamios programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos, atnaujinimo ir kt. reikalavimai nustatomi LIS saugaus elektroninės informacijos tvarkymo taisyklėse;

35.4. turi būti naudojama kompiuterių tinklo filtravimo įranga (užkardos, turinio kontrolės sistemos, įgaliotieji serveriai (angl. *proxy server*) ir kt.). Išsamios kompiuterių tinklo filtravimo įrangos naudojimo nuostatos nustatomos LIS saugaus elektroninės informacijos tvarkymo taisyklėse;

35.5. užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą, turi būti naudojamas šifravimas, virtualus privatusis tinklas, skirtinės linijos, saugus elektroninių ryšių tinklas ar kitos priemonės, kuriomis užtikrinamas saugus elektroninės informacijos perdavimas. Metodų, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą (nuotolinio prisijungimo prie LIS būdai, protokolai, elektroninės informacijos keitimosi formatai, šifravimo, elektroninės informacijos kopijų skaičiaus reikalavimai, reikalavimai teikti ir (ar) gauti elektroninę informaciją automatiniu būdu tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas ir pan.), aprašymai pateikiami LIS saugaus elektroninės informacijos tvarkymo taisyklėse;

35.6. stacionariuosius kompiuterius leidžiama naudoti tik LIS valdytojo ir LIS tvarkytojų patalpose. Nešiojamiesiems kompiuteriams, išnešamiems iš LIS valdytojo ar LIS tvarkytojų patalpų, turi būti taikomos papildomos saugos priemonės (elektroninės informacijos šifravimas, prisijungimo ribojimas ir pan.).

36. Pagrindiniai atsarginių elektroninės informacijos kopijų darymo ir atkūrimo reikalavimai:

36.1. atsarginių elektroninės informacijos kopijų darymo strategija turi būti pasirenkama atsižvelgiant į priimtiną elektroninės informacijos praradimą (angl. *recovery point objetive*) ir priimtiną LIS neveikimo laikotarpį (angl. *recovery time objective*);

36.2. atsarginės elektroninės informacijos kopijos turi būti daromos ir saugomos tokiu mastu, kad LIS veiklos sutrikimo, elektroninės informacijos saugos ir kibernetinio incidento ar elektroninės informacijos vientisumo praradimo atvejais LIS neveikimo laikotarpis nebūtų ilgesnis, nei teisės aktais nustatyta LIS svarbos kategorijai, nurodytai Saugos nuostatų 21 punkte, o elektroninės informacijos praradimas atitiktų priimtinumo kriterijus;

36.3. atsarginės elektroninės informacijos kopijos turi būti daromos automatiškai periodiškai, bet ne rečiau, nei nustatyta LIS saugaus elektroninės informacijos tvarkymo taisyklėse;

36.4. elektroninė informacija atsarginėse elektroninės informacijos kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo atsarginių elektroninės informacijos kopijų) arba turi būti imtasi kitų priemonių, dėl kurių nebūtų galima neteisėtai atkurti elektroninės informacijos;

36.5. atsarginių elektroninės informacijos kopijų laikmenos turi būti žymimos taip, kad jas būtų galima identifikuoti, ir saugomos nedegioje spintoje kitose patalpose, nei yra LIS tarnybinės stotys ar įrenginys, kurio elektroninė informacija buvo nukopijuota, arba kitame pastate.

36.6. periodiškai, bet ne rečiau kaip kartą per pusmetį, turi būti atliekami elektroninės informacijos atkūrimo iš atsarginių kopijų bandymai;

36.7. patekimas į patalpas, kuriose saugomos atsarginės elektroninės informacijos kopijos, turi būti kontroliuojamas.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

37. LIS naudotojų, LIS administratorių, saugos įgaliotinio kvalifikacijos ir patirties reikalavimai:

37.1. LIS naudotojų, administratorių, saugos įgaliotinio kvalifikacija turi atitikti jų pareiginiuose nuostatuose nustatytus reikalavimus;

37.2. LIS naudotojai privalo turėti pagrindinių darbo taikomosiomis kompiuterinėmis programomis įgūdžių, mokėti tvarkyti elektroninę informaciją, būti susipažinę su asmens duomenų tvarkymą, LIS elektroninės informacijos tvarkymą reglamentuojančiais teisės aktais;

37.3. duomenis ir informaciją tvarkantys asmenys privalo laikyti duomenų ir informacijos paslaptį ir būti pasirašę pasižadėjimą ją saugoti. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą;

37.4. LIS saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo principus, tobulinti elektroninės informacijos saugos ir kibernetinio saugumo srities kvalifikaciją, savo darbe vadovautis Lietuvos Respublikos ir Europos Sąjungos teisės aktų, reglamentuojančių elektroninės informacijos saugą ir kibernetinį saugumą, nuostatomis. LIS tvarkytojas turi sudaryti sąlygas kelti LIS saugos įgaliotinio kvalifikaciją.

37.5. LIS administratoriai pagal kompetenciją privalo išmanyti elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo principus, mokėti užtikrinti LIS ir joje tvarkomos elektroninės informacijos saugą ir kibernetinį saugumą, administruoti ir prižiūrėti LIS komponentus (stebėti LIS komponentų veikimą, atlikti jų profilaktinę priežiūrą, trikčių diagnostiką ir šalinimą, sugebėti užtikrinti nepertraukiamą LIS komponentų veikimą ir pan.). LIS administratoriai turi būti susipažinę su Saugos dokumentais.

38. LIS naudotojų ir LIS administratorių mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo dažnumo reikalavimai:

38.1. LIS naudotojams turi būti įvairiais būdais primenama apie elektroninės informacijos saugos ir kibernetinio saugumo problemas (pavyzdžiui, siunčiami priminimai elektroniniu paštu, organizuojami teminiai renginiai, teikiamos atmintinės naujiems LIS naudotojams, LIS administratoriams ir panašiai);

38.2. mokymai elektroninės informacijos saugos ir kibernetinio saugumo klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), saugos įgaliotinio, LIS naudotojų ar LIS administratorių poreikius;

38.3. mokymai gali būti vykdomi tiesioginiu (pavyzdžiui, paskaitos, seminarai, konferencijos ir kiti teminiai renginiai) ar nuotoliniu (pavyzdžiui, vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir panašiai) būdu;

38.4. mokymai LIS naudotojams turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per metus. Už LIS naudotojų mokymų organizavimą atsakingas LIS saugos įgaliotinis;

38.5. mokymai LIS saugos įgaliotiniui ir LIS administratoriams turi būti organizuojami pagal poreikį.

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

39. LIS naudotojų ir LIS administratorių supažindinimą su Saugos dokumentais ar jų santrauka, atsakomybe už Saugos dokumentų nuostatų pažeidimus organizuoja LIS saugos įgaliotinis.

40. LIS naudotojų supažindinimo su Saugos dokumentais ar jų santrauka būdai turi būti pasirenkami atsižvelgiant į LIS specifiką (pavyzdžiui, LIS ir jos naudotojų buvimo vietą organizacinių ir (ar) techninių priemonių, leidžiančių identifikuoti su Saugos dokumentais ar jų santrauka susipažinusį asmenį ir užtikrinančių supažindinimo procedūros įrodomąją (teisinę) galią, panaudojimo galimybes ir panašiai). LIS naudotojai su Saugos dokumentais ar jų santrauka turi būti supažindinami pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodomumą. Saugos dokumentų santrauka išoriniams LIS naudotojams skelbiama LIS tvarkomoje interneto svetainėje ir (ar) LIS taikomosiose programose.

41. Pakartotinai su Saugos dokumentais ar jų santrauka LIS naudotojai supažindinami tik iš esmės pasikeitus informacinei sistemai arba elektroninės informacijos saugą ir kibernetinį saugumą reglamentuojantiems teisės aktams.

42. Tvarkyti ir naudoti LIS elektroninę informaciją gali tik LIS naudotojai, kurie yra susipažinę su Saugos dokumentais ar jų santrauka ir sutikę laikytis šių reikalavimų.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

43. LIS naudotojai, LIS saugos įgaliotinis, LIS administratoriai pagal kompetenciją atsako už LIS tvarkomos elektroninės informacijos saugą ir kibernetinį saugumą, pažeidę Saugos dokumentų ir kitų elektroninės informacijos saugą ir kibernetinį saugumą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

Pakeitimai:

1.
Lietuvos Respublikos ekonomikos ir inovacijų ministerija, Įsakymas
Nr. 4-175, 2022-02-03, paskelbta TAR 2022-02-03, i. k. 2022-01945
Dėl ekonomikos ir inovacijų ministro 2020 m. liepos 21 d. įsakymo Nr. 4-586 „Dėl Licencijų informacinės sistemos duomenų saugos nuostatų patvirtinimo“ pakeitimo