LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTRAS

ĮSAKYMAS DĖL LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTRO 2004 M. GEGUŽĖS 6 D. ĮSAKYMO NR. 1V-156 „DĖL INFORMACINIŲ TECHNOLOGIJŲ SAUGOS ATITIKTIES VERTINIMO METODIKOS PATVIRTINIMO“ PAKEITIMO

2016 m. rugpjūčio 2 d. Nr. 1V-534
Vilnius

P a k e i č i u Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymą Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ ir jį išdėstau nauja redakcija:

„**LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTRAS**

ĮSAKYMAS DĖL INFORMACINIŲ TECHNOLOGIJŲ SAUGOS ATITIKTIES VERTINIMO METODIKOS PATVIRTINIMO

Vadovaudamasis 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 43 punktu,

t v i r t i n u Informacinių technologijų saugos atitikties vertinimo metodiką (pridedama).“

Vidaus reikalų ministras Tomas Žilinskas

PATVIRTINTA
Lietuvos Respublikos vidaus reikalų ministro
2004 m. gegužės 6 d. įsakymu Nr. 1V-156
(Lietuvos Respublikos vidaus reikalų
ministro 2016 m. rugpjūčio 2 d.
įsakymo Nr. 1V-534 redakcija)

INFORMACINIŲ TECHNOLOGIJŲ SAUGOS ATITIKTIES VERTINIMO METODIKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Informacinių technologijų saugos atitikties vertinimo metodika (toliau – Metodika) nustato informacinių technologijų saugos valstybės registruose, žinybiniuose registruose, valstybės informacinėse sistemose ir kitose informacinėse sistemose (toliau – informacinės sistemos) atitikties 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas), Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“, Bendruosiuose reikalavimuose organizacinėms ir techninėms asmens duomenų saugumo priemonėms, patvirtintuose Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) „Dėl Bendrųjų reikalavimų organizacinėms ir techninėms asmens duomenų saugumo priemonėms patvirtinimo“, ir Lietuvos standartuose LST ISO/IEC 27001:2013 ir LST ISO/IEC 27002:2014 nustatytiems elektroninės informacijos saugos reikalavimams vertinimo (toliau – atitikties vertinimas) organizavimo ir atlikimo tvarką.

2. Metodikoje vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme ir Bendrųjų elektroninės informacijos saugos reikalavimų apraše.

II SKYRIUS
ATITIKTIES VERTINIMO TVARKA

3. Atitikties vertinimą gali atlikti informacinės sistemos saugos įgaliotinis, informacinės sistemos valdytojo arba jo pavedimu informacinės sistemos tvarkytojo vidaus auditorius ar kitas

informacinės sistemos valdytojo arba jo pavedimu informacinės sistemos tvarkytojo paskirtas vertintojas (toliau – vertintojas). Vertintojas, atlikdamas atitikties vertinimą, įvertina, kaip informacinės sistemos valdytojas ir (ar) informacinės sistemos tvarkytojas įgyvendina saugos reikalavimus.

4. Atliekant atitikties vertinimą Metodikos 1 punkte nurodytuose teisės aktuose ir standartuose išdėstytų saugos reikalavimų įgyvendinimo lygis nustatomas pagal penkių balų skalę, kurioje žemiausia reikšmė yra vienetas, o aukščiausia – penketas:

4.1. vienetas – saugos reikalavimas ar reikalavimai (toliau – saugos reikalavimai) neįgyvendinti ir nesiimta veiksmų šiems reikalavimams įgyvendinti;

4.2. dvejetas – saugos reikalavimai neįgyvendinti, tačiau imtasi veiksmų šiems reikalavimams įgyvendinti (informacinės sistemos valdytojas ar jo pavedimu informacinės sistemos tvarkytojas, siekdamas įgyvendinti saugos reikalavimus, patvirtino veiksmų planą, parengė teisės akto projektą, investicijų projektą ir pan.);

4.3. trejetas – saugos reikalavimai įgyvendinami tik iš dalies arba nustatyta esminių trūkumų juos įgyvendinant (vertintojo nuomone, labai vėluojama vykdyti Metodikos 1 punkte nurodytuose teisės aktuose ir standartuose bei saugos dokumentuose nustatytas procedūras arba jos iš viso nėra vykdomos, saugos dokumentai nustatytu laiku neperžiūrimi ir (ar) neatnaujinami, nepaskirti atsakingi vykdytojai arba jie nesupažindinti su atitinkamomis procedūromis, įgyvendintos informacinių technologijų saugos priemonės nepasiekia joms keltų tikslų ir pan.);

4.4. ketvertas – saugos reikalavimai įgyvendinami, tačiau nustatyta neesminių trūkumų (vertintojo nuomone, nedaug nukrypstama nuo saugos reikalavimams keliamų kiekybinių rodiklių, nedaug vėluojama vykdyti Metodikos 1 punkte nurodytuose teisės aktuose ir standartuose bei saugos dokumentuose nustatytas procedūras, peržiūrėti ir (ar) atnaujinti saugos dokumentus ir pan.);

4.5. penketas – saugos reikalavimai įgyvendinami visa apimtimi.

5. Atitikties vertinimo metu, siekiant objektyviai nustatyti saugos reikalavimų įgyvendinimo lygį, vertintojui rekomenduojama:

5.1. Inventorizuoti informacinės sistemos techninę ir programinę įrangą:

5.1.1. identifikuoti informacinės sistemos tarnybinių ir darbo stočių išdėstymą;

5.1.2. fiksuoti informacinės sistemos tarnybinių ir darbo stočių technines charakteristikas;

5.1.3. sudaryti ar atnaujinti informacinės sistemos tarnybinių ir darbo stočių inventorizacijos aprašą;

5.2. patikrinti ne mažiau kaip 10 procentų atsitiktinai parinktų informacinės sistemos naudotojų kompiuterizuotų darbo vietų, visose informacinės sistemos tarnybinėse stotyse įdiegtas programas ir jų sąranką:

5.2.1. atlikti informacinės sistemos tarnybinių stočių konfigūracijų patikrą;

5.2.2. peržiūrėti leistinos informacinės sistemos programinės įrangos sąrašą;

5.2.3. patikrinti, ar informacinės sistemos naudotojui nustatytų funkcijų vykdymui reikalinga informacinės sistemos sisteminė ir taikomoji programinė įranga legali ir saugi;

5.2.4. patikrinti, ar įdiegiami operacinių sistemų ir naudojamos taikomosios programinės įrangos gamintojų rekomenduojami atnaujinimai;

5.3. patikrinti (įvertinti) informacinės sistemos naudotojams suteiktų teisių ir vykdomų funkcijų atitiktį:

5.3.1. patikrinti informacinės sistemos naudotojų paskyras, siekiant užtikrinti, kad darbo santykius nutraukusiems asmenims būtų panaikinta prieiga prie informacinės sistemos;

5.3.2. patikrinti prašyme suteikti prieigos teisę nurodytų duomenų ir suteiktų teisių atitiktį;

5.3.3. patikrinti informacinės sistemos naudotojams suteiktų teisių ir pareigybės aprašyme ar kituose dokumentuose, kuriuose nurodomi informacinės sistemos naudotojams suteikti įgaliojimai, nustatytų funkcijų atitiktį, siekiant užtikrinti, kad nebūtų suteiktos neteisėtos prieigos teisės;

5.4. įvertinti pasirengimą užtikrinti informacinės sistemos veiklos tęstinumą įvykus elektroninės informacijos saugos incidentui:

5.4.1. patikrinti, ar laikomasi nustatytos atsarginių elektroninės informacijos kopijų darymo ir atkūrimo tvarkos;

5.4.2. įvertinti, ar, įvykus elektroninės informacijos saugos incidentui, informacinės sistemos personalas pasirengęs įgyvendinti informacinės sistemos veiklos tęstinumo valdymo planą;

5.4.3. patikrinti, ar išbandomas informacinės sistemos veiklos tęstinumo valdymo planas ir ar parengta ataskaita apie pastebėtus plano veiksmingumo trūkumus, įvertinti šių trūkumų šalinimo būklę;

5.5. įvertinti informacinės sistemos rizikos įvertinimo ir valdymo būklę:

5.5.1. patikrinti, ar atliekamas informacinės sistemos rizikos įvertinimas, parengta rizikos įvertinimo ataskaita;

5.5.2. patikrinti, ar patvirtintas informacinės sistemos rizikos įvertinimo ir rizikos valdymo priemonių planas, įvertinti šio plano vykdymą;

5.6. patikrinti, ar informacinės sistemos saugos dokumentai persvarstomi (peržiūrimi) saugos reikalavimuose nustatytu metu, ir įvertinti jų kokybę.

III SKYRIUS
BAIGIAMOSIOS NUOSTATOS

6. Atlikęs atitikties vertinimą, vertintojas atlieka Bendrųjų elektroninės informacijos saugos reikalavimų aprašo 44–45 punktuose nurodytus veiksmus.